Prestige 650HW

ADSL Router

User's Guide

Version 3.40

June 2002

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Copyright

Copyright © 2002 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

Refer to the product page at www.zyxel.com.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.

2. Do not use this product near water, for example, in a wet basement or near a swimming pool.

3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Information in **Menu 24.2.1 – System Information**.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu 300, Taiwan.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A4 D-52146 Wuerselen, Germany
MALAYSIA	support@zyxel.com.my sales@zyxel.com.my	+603-795-44-688 +603-795-34-407	www.zyxel.com.my	Lot B2-06, PJ Industrial Park, Section 13, Jalan Kemajuan, 46200 Petaling Jaya Selangor Darul Ehasn, Malaysia

Table of Contents

Copyright ..... **ii**
Federal Communications Commission (FCC) Interference Statement ..... **iii**
ZyXEL Limited Warranty ..... **iv**
Customer Support ..... **v**
List of Figures ..... **xi**
List of Tables ..... **xiv**
Preface ..... **xvi**
What is DSL? ..... **xviii**
GETTING STARTED ..... **I**
Chapter 1 Getting To Know Your Prestige **1-1**
1.1 Prestige P650HW ADSL Internet Access Router 1-1
1.2 Features of the Prestige P650HW 1-1
1.3 Applications for the Prestige P650HW 1-6
1.3.1 Internet Access 1-6
1.3.2 LAN to LAN Application 1-7
Chapter 2 Hardware Installation and Initial Setup **2-1**
2.1 Front Panel LEDs of the PP650H 2-1
2.2 Rear Panel and Connections of the Prestige P650HW 2-2
2.2.1 DSL Port 2-3
2.2.2 Four LAN 10/100M Ports 2-4
2.2.3 PCMCIA Wireless Card Slot 2-4
2.2.4 Power Port 2-4
2.2.5 Restore Factory Defaults/Reboot Button 2-4
2.3 Additional Installation Requirements 2-4
2.4 P650HW with POTS 2-5
2.4.1 Connecting a POTS Splitter 2-5
2.4.2 Telephone Microfilters 2-6
2.5 P650HW With ISDN 2-6
2.6 Turning On Your Prestige 2-7
2.7 Configuring Your Prestige For Internet Access 2-7
2.7.1 Connect to your Prestige Using Telnet 2-7
2.7.2 Connect to your Prestige Using the Web Configurator 2-8
2.7.3 Entering Password 2-8
2.8 Resetting the Prestige 2-8
2.8.1 Methods of Restoring Factory-Defaults 2-9
2.8.2 Prestige P650HW SMT Menu Overview 2-9
2.9 Navigating the SMT Interface 2-11
2.9.1 System Management Terminal Interface Summary 2-12
2.10 Changing the System Password 2-13

2.11 General Setup 2-13
2.11.1 Dynamic DNS 2-14
2.11.2 Procedure To Configure Menu 1 2-14
2.11.3 Procedure to Configure Dynamic DNS 2-15
2.12 LAN Setup 2-16
2.12.1 General Ethernet Setup 2-17
2.13 Protocol Dependent Ethernet Setup 2-17
Chapter 3 Internet Access 3-1
3.1 Factory Ethernet Defaults 3-1
3.2 LANs and WANs 3-1
3.2.1 LANs, WANs and the Prestige 3-1
3.3 TCP/IP Parameters 3-2
3.3.1 IP Address and Subnet Mask 3-2
3.3.2 Private IP Addresses 3-3
3.3.3 RIP Setup 3-3
3.3.4 DHCP Configuration 3-4
3.4 IP Multicast 3-5
3.5 IP Policies 3-5
3.6 IP Alias 3-5
3.6.1 IP Alias Setup 3-6
3.7 Route IP Setup 3-8
3.8 TCP/IP Ethernet Setup and DHCP 3-8
3.9 Wireless LAN 3-11
3.9.1 Wireless LAN Parameters 3-11
3.9.2 Wireless LAN Setup 3-13
3.9.3 Wireless LAN MAC Address Filter 3-15
3.10 Internet Access Setup 3-16
3.11 VPI and VCI 3-16
3.12 Multiplexing 3-16
3.12.1 VC-based Multiplexing 3-16
3.12.2 LLC-based Multiplexing 3-16
3.13 Encapsulation 3-16
3.13.1 ENET ENCAP 3-16
3.13.2 PPP over Ethernet 3-17
3.13.3 PPP 3-17
3.13.4 RFC 1483 3-17
3.14 IP Address Assignment 3-17
3.14.1 Using PPP or PPPoE Encapsulation 3-17
3.14.2 Using RFC 1483 Encapsulation 3-17
3.14.3 Using ENET ENCAP Encapsulation 3-17
3.15 Internet Access Configuration 3-18

3.15.1 Traffic Shaping 3-19
ADVANCED APPLICATIONS III
Chapter 4 Remote Node Configuration 4-1
4.1 Remote Node Setup 4-1
4.1.1 Remote Node Profile 4-1
4.1.2 Encapsulation and Multiplexing Scenarios 4-2
4.1.3 Outgoing Authentication Protocol 4-6
4.2 Remote Node Setup 4-7
4.3 Remote Node Filter 4-9
Chapter 5 Remote Node TCP/IP Configuration 5-1
5.1 TCP/IP Configuration 5-1
5.1.1 Editing TCP/IP Options 5-1
5.1.2 IP Static Route Setup 5-5
Chapter 6 Bridging Setup 6-1
6.1 Bridging in General 6-1
6.2 Bridge Ethernet Setup 6-1
6.2.1 Remote Node Bridging Setup 6-1
6.2.2 Bridge Static Route Setup 6-2
Chapter 7 Network Address Translation (NAT) 7-1
7.1 Introduction 7-1
7.1.1 NAT Definitions 7-1
7.1.2 What NAT Does 7-2
7.1.3 How NAT Works 7-2
7.1.4 NAT Application 7-3
7.1.5 NAT Mapping Types 7-4
7.2 Using NAT 7-6
7.2.1 SUA (Single User Account) Versus NAT 7-6
7.2.2 Applying NAT 7-6
7.3 NAT Setup 7-8
7.3.1 Address Mapping Sets 7-8
7.4 NAT Server Sets – Port Forwarding 7-14
7.4.1 Configuring a Server behind NAT 7-15
7.5 General NAT Examples 7-18
7.5.1 Example 1: Internet Access Only 7-18
7.5.2 Example 2: Internet Access with an Inside Server 7-19
7.5.3 Example 3: Multiple Public IP Addresses With Inside Servers 7-20
7.5.4 Example 4: NAT Unfriendly Application Programs 7-24
ADVANCED MANAGEMENT III
Chapter 8 Filter Configuration 8-1
8.1 About Filtering 8-1
8.2 Configuring a Filter Set 8-4

8.2.1 Filter Rules Summary Menus 8-7
8.3 Configuring a Filter Rule 8-9
8.3.1 TCP/IP Filter Rule 8-9
8.3.2 Generic Filter Rule 8-14
8.4 Filter Types and NAT 8-16
8.5 Example Filter 8-16
8.6 Applying Filters and Factory Defaults 8-19
8.6.1 Ethernet Traffic 8-20
8.6.2 Remote Node Filters 8-20
Chapter 9 SNMP Configuration 9-1
9.1 About SNMP 9-1
9.2 Supported MIBs 9-2
9.3 SNMP Configuration 9-2
9.4 SNMP Traps 9-4
Chapter 10 System Information and Diagnosis 10-1
10.1 System Status 10-1
10.2 System Information 10-3
10.2.1 System Information 10-4
10.3 Log and Trace 10-5
10.3.1 Viewing Error Log 10-5
10.3.2 Syslog and Accounting 10-6
10.4 Diagnostic 10-8
Chapter 11 Firmware and Configuration File Maintenance 11-1
11.1 Filename Conventions 11-1
11.2 Backup Configuration 11-2
11.2.1 Backup Configuration Using FTP 11-2
11.2.2 Using the FTP command from the DOS Prompt 11-3
11.2.3 Backup Configuration Using TFTP 11-4
11.2.4 Example: TFTP Command 11-5
11.3 Restore Configuration 11-6
11.4 Uploading Firmware and Configuration Files 11-6
11.4.1 Firmware Upload 11-7
11.4.2 Configuration File Upload 11-7
11.4.3 Using the FTP command from the DOS Prompt Example 11-8
11.4.4 TFTP File Upload 11-9
11.4.5 Example: TFTP Command 11-10
Chapter 12 System Maintenance and Information 12-1
12.1 Command Interpreter Mode 12-1
12.2 Call Control Support 12-2
12.2.1 Budget Management 12-2
12.3 Time and Date Setting 12-4

12.3.1 Resetting the Time 12-5
Chapter 13 IP Policy Routing 13-1
13.1 Introduction 13-1
13.2 Benefits 13-1
13.3 Routing Policy 13-1
13.4 IP Routing Policy Setup 13-2
13.5 Applying an IP Policy 13-5
13.5.1 Ethernet IP Policies 13-5
13.6 IP Policy Routing Example 13-8
Chapter 14 Call Scheduling 14-1
14.1 Introduction 14-1
Chapter 15 Remote Management 15-1
15.1 Telnet 15-1
15.2 FTP 15-1
15.3 Web 15-1
15.4 Remote Management 15-1
15.4.1 Remote Management Setup 15-2
15.4.2 Remote Management Limitations 15-3
15.5 Remote Management and NAT 15-3
15.6 System Timeout 15-4
ADDITIONAL INFORMATION 1
Chapter 16 Troubleshooting 16-1
16.1 Problems Starting Up the Prestige 16-1
16.2 Problems with the LAN Interface 16-1
16.3 Problems with the WAN Interface 16-2
16.4 Problems with Internet Access 16-2
16.5 Problems with the Password 16-3
16.6 Problems with Telnet 16-3
Appendix A Wireless LAN and IEEE 802.11 ..... A
Appendix B PPPoE ..... D
Appendix C Virtual Circuit Topology ..... F
Appendix D Power Adapter Specifications ..... G
Appendix E TCP/IP ..... H
Index ..... M

List of Figures

Figure 1-1 Internet Access Application 1-6
Figure 1-2 LAN-to-LAN Application 1-7
Figure 2-1 Prestige P650HW Front Panel 2-1
Figure 2-2 Prestige P650HW Rear Panel and Connections 2-3
Figure 2-3 Connecting a POTS Splitter 2-5
Figure 2-4 Connecting a Microfilter 2-6
Figure 2-5 P650HW with ISDN 2-7
Figure 2-6 Login Screen 2-8
Figure 2-7 Prestige P650HW SMT Menu Overview 2-10
Figure 2-8 SMT Main Menu 2-12
Figure 2-9 Menu 23 — System Password 2-13
Figure 2-10 Menu 1 — General Setup 2-14
Figure 2-11 Configure Dynamic DNS 2-16
Figure 2-12 Menu 3 — LAN Setup 2-17
Figure 2-13 Menu 3.1 — General Ethernet Setup 2-17
Figure 3-1 LAN & WAN IPs 3-2
Figure 3-2 Physical Network 3-6
Figure 3-3 Partitioned Logical Networks 3-6
Figure 3-4 Menu 3.2 — TCP/IP and DHCP Setup 3-6
Figure 3-5 Menu 3.2.1 — IP Alias Setup 3-7
Figure 3-6 Menu 1 — General Setup 3-8
Figure 3-7 Menu 3.2 — TCP/IP and DHCP Ethernet Setup 3-9
Figure 3-8 RTS Threshold 3-12
Figure 3-9 Menu 3.5 - Wireless LAN Setup 3-13
Figure 3-10 Menu 3.5.1- WLAN MAC Address Filtering 3-15
Figure 3-11 Example of Traffic Shaping 3-20
Figure 3-12 Internet Access Setup 3-20
Figure 4-1 Menu 11 — Remote Node Setup 4-2
Figure 4-2 Menu 11.1 — Remote Node Profile 4-4
Figure 4-3 Remote Node Network Layer Options 4-7
Figure 4-4 Menu 11.5 — Remote Node Filter (RFC 1483 or ENET Encapsulation) 4-9
Figure 4-5 Menu 11.5 — Remote Node Filter (PPP or PPPoE Encapsulation) 4-10
Figure 5-1 Menu 11.6 for VC-based Multiplexing 5-2
Figure 5-2 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation 5-2
Figure 5-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection 5-3
Figure 5-4 Remote Node Network Layer Options 5-4
Figure 5-5 Sample Static Routing Topology 5-6
Figure 5-6 Menu 12 — Static Route Setup 5-6
Figure 5-7 Menu 12.1 — IP Static Route Setup 5-7

Figure 5-8 Edit IP Static Route 5-7
Figure 6-1 Menu 11.3 — Remote Node Bridging Options 6-2
Figure 6-2 Menu 12.3.1 — Edit Bridge Static Route 6-3
Figure 7-1 How NAT Works 7-3
Figure 7-2 NAT Application With IP Alias 7-4
Figure 7-3 Menu 4 — Applying NAT for Internet Access 7-6
Figure 7-4 Menu 11.3 — Applying NAT to the Remote Node 7-7
Figure 7-5 Menu 15 — NAT Setup 7-8
Figure 7-6 Menu 15.1 — Address Mapping Sets 7-9
Figure 7-7 Menu 15.1.255 — SUA Address Mapping Rules 7-10
Figure 7-8 Menu 15.1.1 — First Set 7-11
Figure 7-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set 7-13
Figure 7-10 Menu 15.2 — NAT Server Setup 7-16
Figure 7-11 Menu 15.2.1 — NAT Server Setup 7-16
Figure 7-12 Multiple Servers Behind NAT Example 7-17
Figure 7-13 NAT Example 1 7-18
Figure 7-14 Menu 4 — Internet Access & NAT Example 7-18
Figure 7-15 NAT Example 2 7-19
Figure 7-16 Menu 15.2.1 — Specifying an Inside Server 7-20
Figure 7-17 NAT Example 3 7-21
Figure 7-18 Example 3: Menu 11.3 7-22
Figure 7-19 Example 3: Menu 15.1.1.1 7-22
Figure 7-20 Example 3: Final Menu 15.1.1 7-23
Figure 7-21 NAT Example 4 7-24
Figure 7-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule 7-25
Figure 7-23 Example 4: Menu 15.1.1 — Address Mapping Rules 7-26
Figure 8-1 Outgoing Packet Filtering Process 8-2
Figure 8-2 Filter Rule Process 8-3
Figure 8-3 Menu 21 — Filter Set Configuration 8-4
Figure 8-4 NetBIOS_WAN Filter Rules Summary 8-5
Figure 8-5 NetBIOS_LAN Filter Rules Summary 8-5
Figure 8-6 Telnet_WAN Filter Rules Summary 8-6
Figure 8-7 PPPoE Filter Rules Summary 8-6
Figure 8-8 FTP_WAN Filter Rules Summary 8-7
Figure 8-9 WebSet Filter Rules Summary 8-7
Figure 8-10 Menu 21.1.1 — TCP/IP Filter Rule 8-10
Figure 8-11 Executing an IP Filter 8-13
Figure 8-12 Menu 21.5.1 — Generic Filter Rule 8-14
Figure 8-13 Protocol and Device Filter Sets 8-16
Figure 8-14 Sample Telnet Filter 8-17
Figure 8-15 Sample Filter — Menu 21.3.1 8-18

Figure 8-16 Sample Filter Rules Summary — Menu 21.1 8-19
Figure 8-17 Filtering Ethernet Traffic 8-20
Figure 8-18 Filtering Remote Node Traffic 8-21
Figure 9-1 SNMP Management Model 9-1
Figure 9-2 Menu 22 — SNMP Configuration 9-3
Figure 10-1 Menu 24 — System Maintenance 10-1
Figure 10-2 Menu 24.1 — System Maintenance — Status 10-2
Figure 10-3 Menu 24.2 — System Information and Console Port Speed 10-3
Figure 10-4 Menu 24.2.1 — System Maintenance — Information 10-4
Figure 10-5 Menu 24.3 — System Maintenance — Log and Trace 10-5
Figure 10-6 Sample Error and Information Messages 10-5
Figure 10-7 Menu 24.3.2 — System Maintenance — Syslog and Accounting 10-6
Figure 10-8 Menu 24.4 — System Maintenance — Diagnostic 10-8
Figure 11-1 Menu 24.5 — Backup Configuration 11-3
Figure 11-2 FTP Session Example 11-3
Figure 11-3 Menu 24.6 — Restore Configuration 11-6
Figure 11-5 Menu 24.7 — System Maintenance — Upload Firmware 11-7
Figure 11-6 Menu 24.7.1 — Upload System Firmware 11-7
Figure 11-7 Menu 24.7.2 — System Maintenance 11-8
Figure 11-8 FTP Session Example 11-9
Figure 12-1 Command Mode in Menu 24 12-1
Figure 12-2 Valid Commands 12-2
Figure 12-3 Call Control 12-2
Figure 12-4 Budget Management 12-3
Figure 12-5 Menu 24 — System Maintenance 12-4
Figure 12-6 Menu 24.10 System Maintenance — Time and Date Setting 12-4
Figure 13-1 IP Routing Policy Setup 13-2
Figure 13-2 Menu 25.1 — Sample IP Routing Policy Setup 13-3
Figure 13-3 IP Routing Policy 13-4
Figure 13-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup 13-7
Figure 13-5 Menu 11.3 — Remote Node Network Layer Options 13-7
Figure 13-6 Example of IP Policy Routing 13-8
Figure 13-7 IP Routing Policy Example 13-9
Figure 13-8 IP Routing Policy 13-10
Figure 13-9 Applying IP Policies 13-10
Figure 14-1 Menu 26 — Schedule Setup 14-1
Figure 14-2 Schedule Set Setup 14-2
Figure 14-3 Applying Schedule Set(s) to a Remote Node (PPPoE) 14-4
Figure 15-1 Telnet Configuration on a TCP/IP Network 15-1
Figure 15-2 Menu 24.11 — Remote Management Control 15-2

List of Tables

Table 2-1 Front Panel LED Description 2-1
Table 2-2 Main Menu Commands 2-11
Table 2-3 Main Menu Summary 2-12
Table 2-4 General Setup Menu Fields 2-15
Table 2-5 Configure Dynamic DNS Menu Fields 2-16
Table 3-1 IP Alias Setup Menu Fields 3-7
Table 3-2 DHCP Ethernet Setup Menu Fields 3-9
Table 3-3 TCP/IP Ethernet Setup Menu Fields 3-10
Table 3-4 Wireless LAN Setup Field Description 3-13
Table 3-5 MAC Address Filter Field Description 3-15
Table 3-6 Internet Account Information 3-18
Table 3-7 Internet Access Setup Menu Fields 3-21
Table 4-1 Remote Node Profile Menu Fields 4-4
Table 4-2 Remote Node Network Layer Options 4-7
Table 5-1 TCP/IP-Related Fields in Menu 11.1 — Remote Node Profile 5-3
Table 5-2 TCP/IP Remote Node Configuration 5-4
Table 5-3 Edit IP Static Route Menu Fields 5-7
Table 6-1 Remote Node Bridge Options 6-2
Table 6-2 Edit Bridge Static Route Menu Fields 6-3
Table 7-1 NAT Definitions 7-1
Table 7-2 NAT Mapping Types 7-5
Table 7-3 Applying NAT in Menus 4 & 11.3 7-7
Table 7-4 SUA Address Mapping Rules 7-10
Table 7-5 Fields in Menu 15.1.1 7-12
Table 7-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set 7-13
Table 7-7 Services & Port Numbers 7-15
Table 8-1 Abbreviations Used in the Filter Rules Summary Menu 8-8
Table 8-2 Rule Abbreviations Used 8-8
Table 8-3 TCP/IP Filter Rule Menu Fields 8-10
Table 8-4 Generic Filter Rule Menu Fields 8-15
Table 8-5 Filter Sets Table 8-20
Table 9-1 SNMP Configuration Menu Fields 9-3
Table 9-2 SNMP Traps 9-4
Table 9-3 Ports and Permanent Virtual Circuits 9-4
Table 10-1 System Maintenance — Status Menu Fields 10-2
Table 10-2 Fields in System Maintenance 10-4
Table 10-3 System Maintenance Menu — Syslog Parameters 10-6
Table 10-4 System Maintenance Menu — Diagnostic 10-8
Table 11-1 Filename Conventions 11-2

Table 11-2 General Commands for Third Party FTP Clients 11-4
Table 11-3 General Commands for Third Party TFTP Clients 11-5
Table 12-1 Budget Management 12-3
Table 12-2 Time and Date Setting Fields 12-5
Table 13-1 IP Routing Policy Setup 13-3
Table 13-2 IP Routing Policy 13-4
Table 14-1 Schedule Set Setup Fields 14-2
Table 15-1 Menu 24.11 — Remote Management Control 15-2
Table 16-1 Troubleshooting the Start-Up of Your Prestige 16-1
Table 16-2 Troubleshooting the LAN Interface 16-1
Table 16-3 Troubleshooting the WAN Interface 16-2
Table 16-4 Troubleshooting Internet Access 16-2
Table 16-5 Troubleshooting the Password 16-3
Table 16-6 Troubleshooting Telnet 16-3

Preface

There are two Prestige 650HW models, one for ADSL over POTS (Plain Old Telephone System) and one for ADSL over ISDN (Integrated Synchronous Digital System). Both models are discussed together in this guide.

The P650HW ADSL router is the ideal all-in-one device for small networks connecting to the Internet via ADSL. You don't need to buy an external hub. The P650HW is equipped with four auto-sensing 10/100BASE-T Ethernet ports to connect to your network and an RJ-11 port (POTS) or RJ-45 port (ISDN) to connect to your ADSL service.

The P650HW's 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network using either a crossover or straight-through Ethernet cable.

The P650HW comes with a PCMCIA wireless card slot for an optional 802.11b wireless card that provides wireless LAN connection without the expensive network cabling infrastructure.

The Prestige 650HW is interoperable with all major DSLAM solutions vendors. The P650HW can run maximum upstream transmission rates of up to 832Kbps and maximum downstream transmission rates of 8Mbps. The actual rate depends on the copper category of your telephone wire, distance from the central office and the type of ADSL service subscribed to. See the *What is DSL* section for more background information on DSL and ADSL

In addition, the Prestige 650HW has bridging and IP routing to support a wide range of applications for high-speed Internet access.

Your Prestige is easy to install and configure. All functions are configurable via the SMT (System Management Terminal) and web configurator. Advanced users may configure the Prestige using CLI (Command Line Interface) commands.

Don't forget to register your Prestige (fast, easy online registration at www.zyxel.com) for free future product updates and information.

About This User's Guide

This user's guide covers all aspects of Prestige operations and shows you how to get the best out of the multiple advanced features of your ADSL Router using the SMT. It is designed to guide you through the correct configuration of your Prestige 650H for various applications.

Related Documentation

- Supporting Disk

  More detailed information and examples can be found in our included disk (as well as on the zyxel.com web site). This disk contains information on configuring your Prestige for Internet

Access, general and advanced FAQs, Application Notes, Troubleshooting, a reference for CI Commands and bundled software.

- Read Me First

  Our Read Me First is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- ZyXEL Web Site

  The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

- "Type" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to select one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The Prestige 650HW may be referred to as the P650HW or the Prestige in this user's guide. These names refer to both Prestige 650HW models (ADSL over POTS and ADSL over ISDN) unless specifically identified.

The following section offers some background information on DSL. Skip to *Chapter 1* if you wish to begin working with your router right away.

What is DSL?

DSL (Digital Subscriber Line) technology enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies.

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). Asymmetrical services (ADSL) are suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds.

A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

What is ADSL?

It is an asymmetrical technology, meaning that the downstream data rate is much higher than the upstream data rate. As mentioned, this works well for a typical Internet session in which more information is downloaded, for example, from Web servers, than is uploaded. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable.

Part I:

GETTING STARTED

This part is structured as a step-by-step guide to help you connect, install and set up your Prestige to operate on your network and to access the Internet. Described are Key Features and Applications, Hardware Installation, Initial Setup, Internet Access and Wireless LAN Setup.

Chapter 1
Getting To Know Your Prestige

This chapter describes the key features and applications of your Prestige.

1.1 Prestige P650HW ADSL Internet Access Router

Your Prestige integrates a high-speed 10/100Mbps auto-negotiating LAN interface, a PCMCIA wireless card slot and one high-speed ADSL port into a single package. The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. By integrating DSL, WLAN and NAT, P650HW provides ease of installation and Internet access. What's more, with the wireless LAN connectivity, users can enjoy the convenience and mobility, working anywhere within the coverage area.

1.2 Features of the Prestige P650HW

Your Prestige is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

- **High Speed Internet Access**

Your Prestige ADSL router can support downstream transmission rates of up to 8Mbps and upstream transmission rates of 832 Kbps.

- **IEEE 802.11b 11 Mbps Wireless LAN**

The 11 Mbps wireless LAN provides mobility and a fast network environment for small and home offices. Computers with wireless NICs can connect to the local area network without any wiring efforts and enjoy reliable high-speed connectivity.

- **Wireless LAN MAC Address Filtering**

MAC Address Filtering together with ESSID (Extended Service Set IDentifier) and WEP (Wired Equivalent Privacy) ensure the most secure wireless solution avaliable.

- **PPPoE Support (RFC2516)**

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the Prestige is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

- **NAT for Single-IP-address Internet Access**

The Prestige's SUA (Single User Account) feature allows multiple-user Internet access for the cost of a single IP account. NAT supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealPlayer, VDOLive, Quake, and PPTP. No configuration is needed to support these applications.

- **10/100M Auto-negotiation Ethernet/Fast Ethernet Interface**

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

- **Dynamic DNS Support**

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS client.

- **Multiple PVC (Permanent Virtual Circuits) Support**

Your Prestige supports up to 8 PVC's.

- **ADSL Transmission Rate Standards**

  - Full-Rate (ANSI T1.413, Issue 2; G.dmt (G.992.1) with line rate support of up to 8 Mbps downstream and 832 Kbps upstream.
  - G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream.

- Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.994.1; G.996.1; G.991.1;G.lite (G992.2)).
- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ATM Forum UNI 3.1/4.0 PVC.
- Supports up to 8 PVCs (UBR, CBR).
- Multiple Protocol over AAL5 (RFC 1483).
- PPP over AAL5 (RFC 2364).
- PPP over Ethernet over AAL5 (RFC 2516).
- RFC 1661.
- PPP over PAP (RFC 1334).
- PPP over CHAP (RFC 1994).

- **Protocol Support**

  - DHCP Support

    DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The Prestige can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

  - IP Alias

    IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

  - IP Policy Routing (IPPR)

    Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default

routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

- PPP (Point-to-Point Protocol) link layer protocol.
- Transparently bridging for unsupported network layer protocols.
- RIP I/RIP II
- IGMP Proxy
- ICMP support
- ATM QoS support
- MIB II support (RFC 1213)

- **Networking Compatibility**

Your Prestige is compatible with the major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers, making configuration as simple as possible for you.

- **Multiplexing**

The Prestige Series supports VC-based and LLC-based multiplexing.

- **Encapsulation**

The Prestige Series supports PPP (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM, MAC encapsulated routing (ENET encapsulation) as well as PPP over Ethernet (RFC 2516).

Network Management

- Menu driven SMT (System Management Terminal) management
- Embedded Web Configurator
- CLI (Command Line Interpreter)
- Remote SMT session via Telnet
- Remote Management via Telnet, FTP or Web servers.

- SNMP manageable
- DHCP Server/Client
- Built-in Diagnostic Tools
- Syslog
- Telnet Support (Password-protected telnet access to internal configuration manager)
- TFTP/FTP server, firmware upgrade and configuration backup/support supported
- Supports OAM F4/F5 loop-back, AIS and RDI OAM cells

- **Other PPPoE Features**
  - PPPoE idle time out
  - PPPoE Dial on Demand

- **Diagnostics Capabilities**
  - The Prestige can perform self-diagnostic tests. These tests check the integrity of the following circuitry:
  - FLASH memory
  - ADSL circuitry
  - RAM
  - LAN port

- **Filters**

The Prestige's packet filtering functions allows added network security and management.

- **Ease of Installation**

Your Prestige is designed for quick, intuitive and easy installation.

- **Housing**

Your Prestige's all new compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

1.3 Applications for the Prestige P650HW

1.3.1 Internet Access

The Prestige is the ideal high-speed Internet access solution. Your Prestige supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (for example, T1, OC3, DS3, ATM or Frame Relay). Think of it as the equivalent of a modem rack for ADSL. In addition, you can insert an optional wireless PCMICA card into the P650HW and allow wireless clients access to your LAN resources. A typical Internet Access application is shown below.

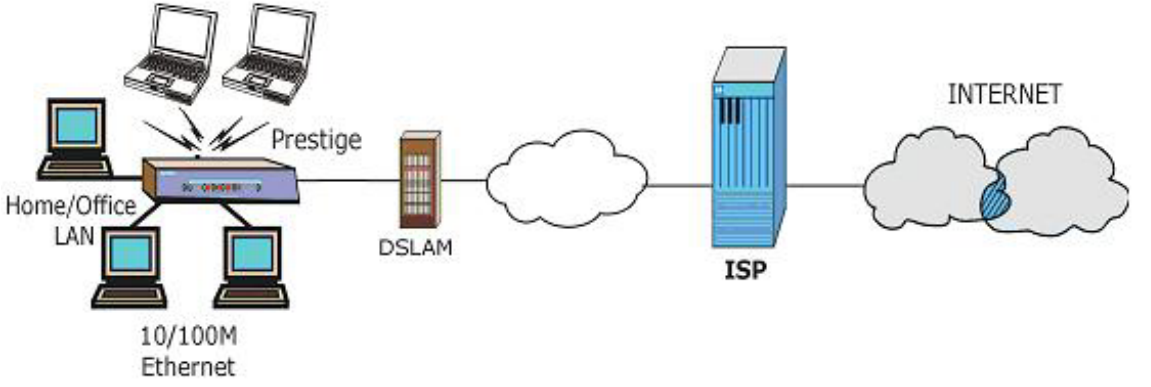

Figure 1-1 Internet Access Application

Internet Single User Account

For a SOHO (Small Office/Home Office) environment, your Prestige offers the Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single IP address.

1.3.2 LAN to LAN Application

You can use the Prestige to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application for your Prestige is shown as follows.

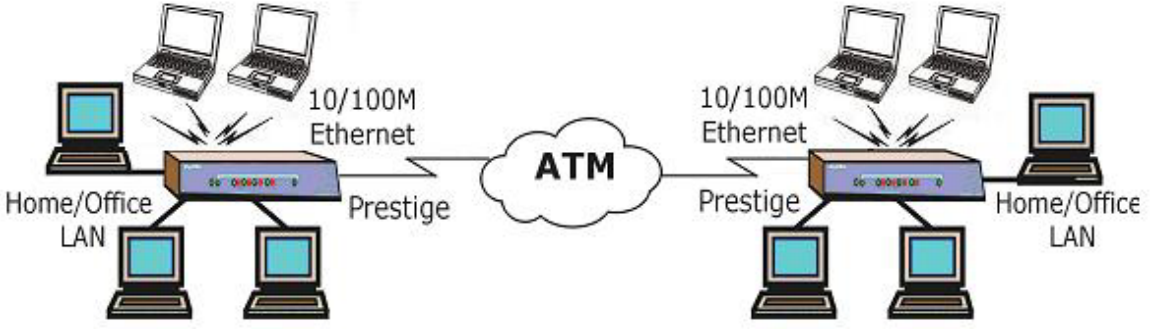

Figure 1-2 LAN-to-LAN Application

Chapter 2
Hardware Installation and Initial Setup

This chapter describes the physical features of the Prestige and how to make cable connections.

2.1 Front Panel LEDs of the PP650H

The LEDs on the front panel indicate the operational status of your Prestige

Figure 2-1 Prestige P650HW Front Panel

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Prestige is receiving power.
		Blinking	The Prestige is performing a self-test.
		Off	The Prestige is not receiving power.
SYS	Green	On	The Prestige is functioning properly.
		Blinking	The Prestige is rebooting.
		Off	The system is not ready or has malfunctioned.
PPPoE	Green	On	The connection to the PPPoE server is up.
		Off	There is no connection to the PPPoE server.
LAN 1-4	Green	On	The Prestige has a successful 10Mb Ethernet connection.

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
		Blinking	The Prestige is sending/receiving data.
		Off	The Prestige does not have 10Mb Ethernet connection.
	Amber	On	The Prestige has a successful 100Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
		Off	The Prestige does not have 100Mb Ethernet connection.
WLAN	Green	On	The Prestige has successful connection to a WLAN.
		Off	WLAN link is not ready or has failed.
		Blinking	The Prestige is sending/receiving data through the WLAN.
DSL	Green	On	The Prestige is linked successfully to a DSLAM.
		Blinking	The Prestige is initializing the DSL line.
		Off	The DSL link is down.
ACT	Green	Blinking	The Prestige is sending/receiving data.
		Off	The system is ready, but is not sending/receiving data.

2.2 Rear Panel and Connections of the Prestige P650HW

The following figure shows the rear panel of your Prestige.

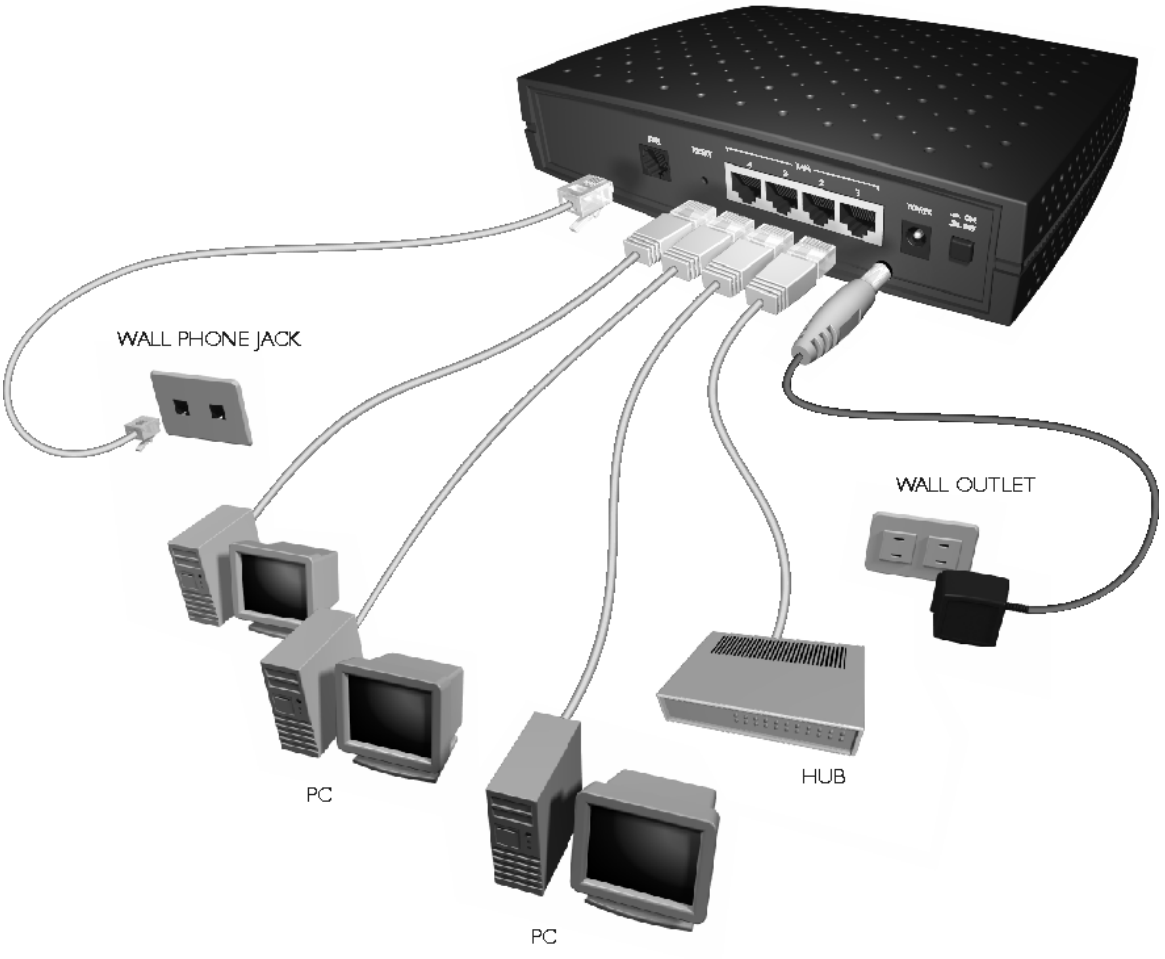

Figure 2-2 Prestige P650HW Rear Panel and Connections

2.2.1 DSL Port

Connect the Prestige directly to the wall jack using the included DSL cable. Connect a microfilter(s) between the wall jack and your telephone(s). A microfilter acts as low-pass filter (voice transmission takes place in the 0 to 4KHz bandwidth) and is an optional purchase.

2.2.2 Four LAN 10/100M Ports

Ethernet 10Base-T/100Base-T networks use Shielded Twisted Pair (STP) cable with RJ-11 (POTS) connectors or RJ-45 (ISDN) connectors that look like a bigger telephone plug with 8 pins. All LAN ports are auto-sensing, so you may use the crossover cable provided or a straight-through Ethernet cable to connect your Prestige to a computer/external hub.

When the Prestige is on and properly connected to a computer or a hub, the corresponding LAN LED on the front panel turns on.

2.2.3 PCMCIA Wireless Card Slot

Your Prestige comes with a PCMCIA wireless LAN card slot for wireless LAN connectivity. Follow the steps below to insert the optional PCMCIA wireless LAN card.

Step 1. Locate the slot on your Prestige.

Step 2. With its 64-pin connector facing the card slot and its label side facing upwards, slide the PCMCIA wireless LANcard into the slot.

Never force, bend or twist the wireless LAN card into the slot.

2.2.4 Power Port

Connect the power adapter to the port labeled POWER on the rear panel of your Prestige. Push in the power button when you want to turn on the Prestige.

To avoid damage to the Prestige, make sure you use the supplied power adapter. Refer to the *Power Adapter Specification Appendix* for this information.

2.2.5 Restore Factory Defaults/Reboot Button

Hold this button in for between 1 and 3 seconds to restart the Prestige.

Upload the default configuration file by holding this button in for more than 3 seconds. Refer to section *2.8* for information on the resetting your Prestige.

2.3 Additional Installation Requirements

- An optional PCMCIA wireless card for 802.11b wireless LAN connection for your P650HW.
- A computer with an Ethernet 10Base-T/100Base-T NIC (Network Interface Card) or a 802.11b wireless LAN card.
- A computer equipped with a web browser (enable JavaScript) and/or Telnet.

2.4 P650HW with POTS

Sections *2.4.1 and 2.4.2* relate to people who use their P650HW with ADSL over POTS (analog telephone service) only.

2.4.1 Connecting a POTS Splitter

This is for the Prestige that follows the Full Rate (G.dmt) standard only. One major difference between ADSL and dial-up modems is the optional telephone splitter. This device keeps the telephone and ADSL signals separated, giving them the capability to provide simultaneous Internet access and telephone service on the same line. Splitters also eliminate the destructive interference conditions caused by telephone sets. The purchase of a POTS splitter is optional.

Noise generated from a telephone in the same frequency range, as the ADSL signal can be disruptive to the ADSL signal. In addition the impedance of a telephone when off-hook may be so low that it shunts the strength of the ADSL signal. When a POTS splitter is installed at the entry point, where the line comes into the home, it will filter the telephone signals before combining the ADSL and telephone signals transmitted and received. The issues of noise and impedance are eliminated with a single POTS splitter installation.

A telephone splitter is easy to install as shown in the following figure.

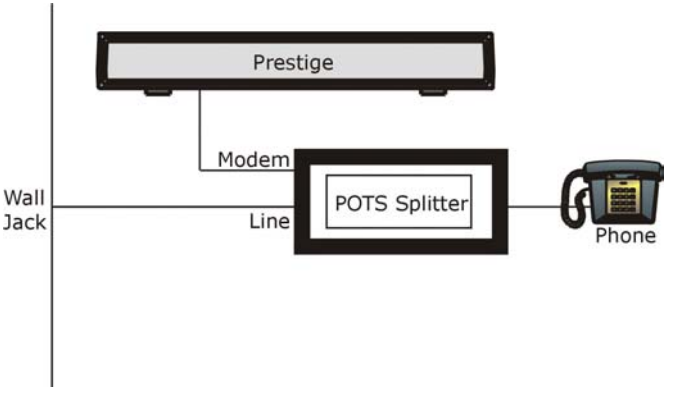

Figure 2-3 Connecting a POTS Splitter

Step 1. Connect the side labeled “Phone” to your telephone.

Step 2. Connect the side labeled “Modem” to your Prestige.

Step 3. Connect the side labeled “Line” to the telephone wall jack.

2.4.2 Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The purchase of a telephone microfilter is optional.

Step 1. Connect a phone cable from the wall jack to the single jack end of the Y- Connector.

Step 2. Connect a cable from the double jack end of the Y-Connector to the "wall side" of the microfilter.

Step 3. Connect another cable from the double jack end of the Y-Connector to the Prestige.

Step 4. Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

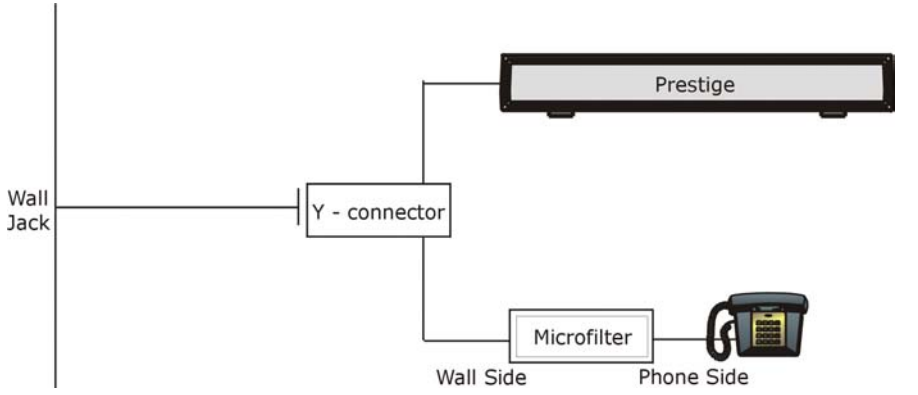

Figure 2-4 Connecting a Microfilter

2.5 P650HW With ISDN

This section relates to people who use their P650HW with ADSL over ISDN (digital telephone service) only. The following is an example installation for the P650HW with ISDN.

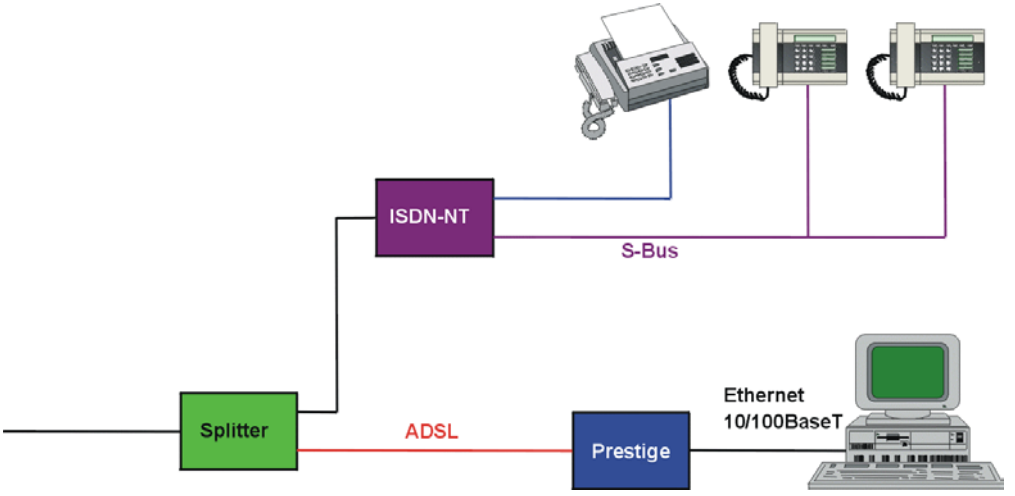

Figure 2-5 P650HW with ISDN

2.6 Turning On Your Prestige

At this point, you should have connected the ADSL line, the Ethernet port and the power port to the appropriate devices or lines. Push in the power button (located on the back of your Prestige) to turn on your Prestige.

2.7 Configuring Your Prestige For Internet Access

Configure your Prestige for Internet access using:

- Web configurator (refer to the *Read Me First*).
- SMT (System Management Terminal). Access the SMT via LAN or WAN using Telnet.

2.7.1 Connect to your Prestige Using Telnet

The following procedure details how to telnet into your Prestige.

Step 1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.

Step 2. Enter "1234" in the **Password** field.

Step 3. After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

2.7.2 Connect to your Prestige Using the Web Configurator

Step 1. Launch your web browser.

Step 2. Enter "192.168.1.1" as the URL.

Step 3. In the **User Name** field, type "admin". In the **Password** field, type "1234". Click **OK**.

Click the **Help** button for online web configurator HTML help.

The remainder of this user's guide shows you how to configure the Prestige for Internet access using SMT screens. There are also some sections in this guide that also focus on using Telnet to configure the Prestige.

2.7.3 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "1234". As you type the password, the screen displays an "X" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out and will display a blank screen. If you see a blank screen, press [ENTER] to display the login screen again.

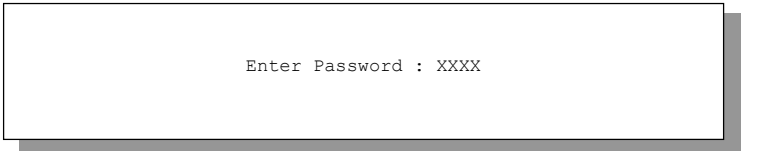

Figure 2-6 Login Screen

2.8 Resetting the Prestige

If you forget your password or cannot access the Prestige, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously; the password will be reset to "1234" and the LAN IP address to 192.168.1.1.

To obtain the default configuration file, download it from the ZyXEL FTP site, unzip it and save it in a folder.

2.8.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in three ways:

1. Transfer the configuration file to your Prestige using the SMT menus. See later in this User's Guide for more information on this.
2. Use the **Restore Factory Defaults/Reboot** button on the rear panel of the Prestige to upload the default configuration file (hold this button in for more than 3 seconds). Use this method for cases when the password or IP address of the Prestige is not known.
3. Use the web configurator to restore defaults (see the web configurator HTML help)

2.8.2 Prestige P650HW SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your Prestige.

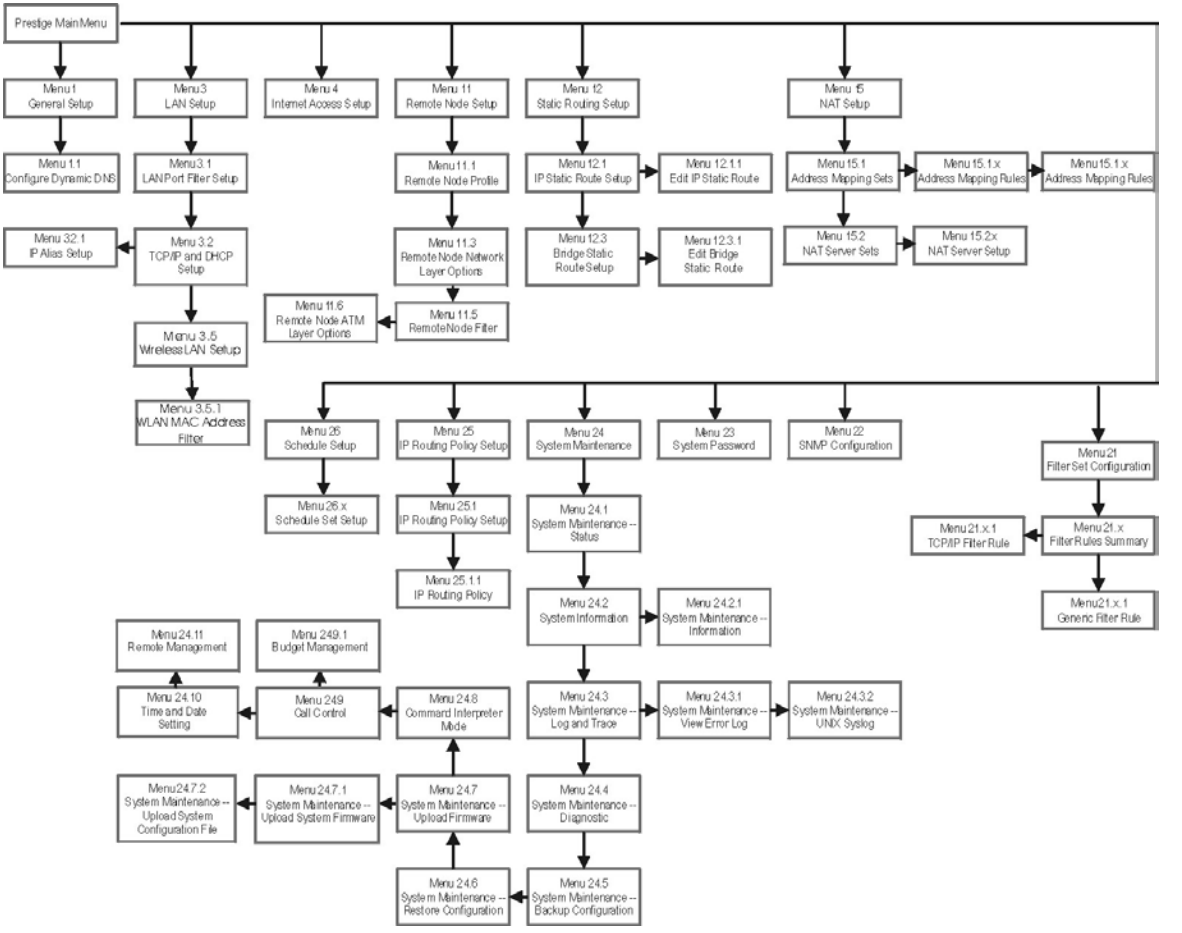
Prestige Main Menu
Menu 1 General Setup
Menu 1.1 Configure Dynamic DNS
Menu 3 LAN Setup
Menu 3.1 LAN Port Filter Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.5 Wireless LAN Setup
Menu 3.5.1 WLAN MAC Address Filter
Menu 32.1 IP Alias Setup
Menu 4 Internet Access Setup
Menu 11 Remote Node Setup
Menu 11.1 Remote Node Profile
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 11.6 Remote Node ATM Layer Options
Menu 12 Static Routing Setup
Menu 12.1 IP Static Route Setup
Menu 12.1.1 Edit IP Static Route
Menu 12.3 Bridge Static Route Setup
Menu 12.3.1 Edit Bridge Static Route
Menu 15 NAT Setup
Menu 15.1 Address Mapping Sets
Menu 15.1.x Address Mapping Rules
Menu 15.1.x Address Mapping Rules
Menu 15.2 NAT Server Sets
Menu 15.2x NAT Server Setup
Menu 26 Schedule Setup
Menu 26.x Schedule Set Setup
Menu 25 IP Routing Policy Setup
Menu 25.1 IP Routing Policy Setup
Menu 25.1.1 IP Routing Policy
Menu 24 System Maintenance
Menu 24.1 System Maintenance -- Status
Menu 24.2 System Information
Menu 24.2.1 System Maintenance -- Information
Menu 24.3 System Maintenance -- Log and Trace
Menu 24.3.1 System Maintenance -- View Error Log
Menu 24.3.2 System Maintenance -- UNIX Syslog
Menu 24.4 System Maintenance -- Diagnostic
Menu 24.5 System Maintenance -- Backup Configuration
Menu 24.6 System Maintenance -- Restore Configuration
Menu 24.7 System Maintenance -- Upload Firmware
Menu 24.7.1 System Maintenance -- Upload System Firmware
Menu 24.7.2 System Maintenance -- Upload System Configuration File
Menu 24.8 Command Interpreter Mode
Menu 24.9 Call Control
Menu 24.9.1 Budget Management
Menu 24.10 Time and Date Setting
Menu 24.11 Remote Management
Menu 23 System Password
Menu 22 SNMP Configuration
Menu 21 Filter Set Configuration
Menu 21.x Filter Rules Summary
Menu 21.x.1 TCP/IP Filter Rule
Menu 21.x.1 Generic Filter Rule

Figure 2-7 Prestige P650HW SMT Menu Overview

2.9 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 2-2 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

```
            Copyright (c) 1994 - 2002 ZyXEL Communications Corp.

                        Prestige 650HW Main Menu

Getting Started                     Advanced Management
    1. General Setup                  21. Filter Set Configuration
    3. LAN Setup                      22. SNMP Configuration
    4. Internet Access Setup          23. System Password
                                      24. System Maintenance
Advanced Applications                 25. IP Routing Policy Setup
   11. Remote Node Setup              26. Schedule Setup
   12. Static Routing Setup
   15. NAT Setup                      99. Exit

                    Enter Menu Selection Number:_
```

Figure 2-8 SMT Main Menu

The SMT menu continually improves and changes with new firmware upgrades. Check the release notes at www.zyxel.com to find the most recent upgrades and information.

2.9.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	LAN Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter Set Configuration	Use this menu to set up filters to provide security, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

2.10 Changing the System Password

Change the Prestige default password by following the steps shown next.

Step 1. Enter 23 in the main menu to display **Menu 23 - System Password** as shown next.

Step 2. Type your existing system password in the **Old Password** field, for example "1234", and press [ENTER].

```
                Menu 23 - System Password

        Old Password= ?
        New Password= ?
        Retype to confirm= ?



         Enter here to CONFIRM or ESC to CANCEL:
```

Figure 2-9 Menu 23 — System Password

Step 3. Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

Step 4. Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an "*" for each character you type.

2.11 General Setup

Menu 1 — General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start** -> **Settings** -> **Control Panel** -> **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows 2000 click **Start**->**Settings**->**Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows XP, click **start** -> **My Computer** -> **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

2.11.1 Dynamic DNS

Dynamic DNS (Domain Name System) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe or other services). You can also access your FTP server or Web site on your own computer using a DNS-like address (for example, *myhost.dhs.org*, where *myhost* is a name of your choice) which will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name.

To use this service, you must register with the Dynamic DNS service provider. The Dynamic DNS service provider will give you a password or key. The Prestige supports www.dyndns.org. You can apply to this service provider for Dynamic DNS service.

DYNDNS Wildcard

Enabling the wildcard feature for your host causes **.yourhost.dyndns.org* to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

2.11.2 Procedure To Configure Menu 1

Step 1. Enter 1 in the Main Menu to open **Menu 1 — General Setup** (shown next).

```
                Menu 1 - General Setup

        System Name= ?
        Location=
        Contact Person's Name=
        Domain Name=
        Edit Dynamic DNS= No

        Route IP= Yes
        Bridge= No
         Press ENTER to Confirm or ESC to Cancel:
```

Figure 2-10 Menu 1 — General Setup

Step 2. Fill in the required fields. Refer to the table shown next for more information about these fields.

Table 2-4 General Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	PP650H
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
Edit Dynamic DNS	Press the [SPACE BAR] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1 — Configure Dynamic DNS** (discussed next).	**No**
Route IP	Set this field to **Yes** to enable or **No** to disable IP routing. You must enable IP routing for Internet access.	**Yes**
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous **Route IP** field. Select **Yes** to turn bridging on; select **No** to turn bridging off.	**No**

2.11.3 Procedure to Configure Dynamic DNS

Step 1. To configure Dynamic DNS, go to **Menu 1 — General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** as shown next.

```
                    Menu 1.1 - Configure Dynamic DNS

      Service Provider = WWW.DynDNS.ORG
      Active= Yes
      Host= me.ddns.org
      EMAIL= mail@mailserver
      USER= username
      Password= *********
      Enable Wildcard= No

                Press ENTER to confirm or ESC to cancel:
```

Figure 2-11 Configure Dynamic DNS

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 2-5 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
Host	Enter the domain name assigned to your Prestige by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	**No**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

If you have a private WAN IP address, then you cannot use Dynamic DNS.

2.12 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3.

```
                    Menu 3 - LAN Setup


          1. LAN Port Filter Setup
          2. TCP/IP and DHCP Setup

          5. Wireless LAN Setup


               Enter Menu Selection Number:
```

Figure 2-12 Menu 3 — LAN Setup

2.12.1 General Ethernet Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

```
                Menu 3.1 - LAN Port Filter Setup

          Input Filter Sets:
            protocol filters=
            device filters=
          Output Filter Sets:
            protocol filters=
            device filters=

          Press ENTER to Confirm or ESC to Cancel:
```

Figure 2-13 Menu 3.1 — General Ethernet Setup

If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

2.13 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to *Internet Access Application*.
- For bridging Ethernet setup refer to *Bridging Setup*.

Chapter 3
Internet Access

This chapter shows you how to configure the LAN and WAN of your Prestige for Internet access.

3.1 Factory Ethernet Defaults

The Ethernet parameters of the Prestige are preset in the factory with the following values:

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If the parameters are satisfactory, you can skip to *TCP/IP Ethernet Setup and DHCP* to enter the DNS server address(es) if your ISP gives you explicit DNS server address(es). If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

3.2 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

3.2.1 LANs, WANs and the Prestige

The actual physical connection determines whether the Prestige ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside: the WAN network as shown next:

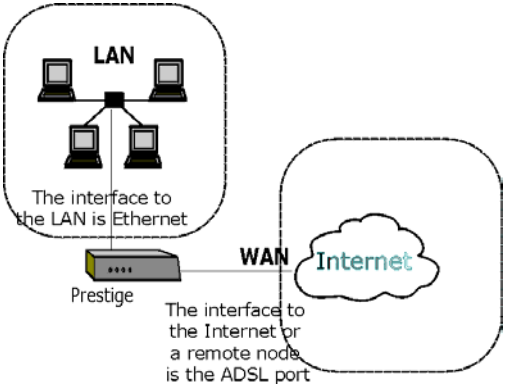
LAN
The interface to the LAN is Ethernet
WAN
Internet
Prestige
The interface to the Internet or a remote node is the ADSL port

Figure 3-1 LAN & WAN IPs

3.3 TCP/IP Parameters

3.3.1 IP Address and Subnet Mask

Like houses on a street that share a common street name, the computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (ignoring the trailing zero) and you must enable the Single User Account feature of the Prestige. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

The subnet mask specifies the network number portion of an IP address. Your Prestige will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Prestige unless you are instructed to do otherwise.

3.3.2 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0      –  10.255.255.255

172.16.0.0    –  172.31.255.255

192.168.0.0   –  192.168.255.255
```

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

3.3.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

1. **Both -** the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only -** the Prestige will not send any RIP packets but will accept all RIP packets received.
3. **Out Only -** the Prestige will send out RIP packets but will not accept any RIP packets received.
4. **None -** the Prestige will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

3.3.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64 for the client machines. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, for example, server for mail, FTP, telnet, web, etc., that you may have.

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Prestige supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are not specified, for instance, left as 0.0.0.0, the Prestige tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the Prestige, the Prestige forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** menu. This way, the Prestige can pass the DNS servers to the computers and the computers can query the DNS server directly without the Prestige's intervention.

3.4 IP Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender – 1 recipient) or Broadcast (1 sender – everybody on the network). Multicast is a third way to deliver IP packets to *a group* of hosts on the network - not everybody.

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP Multicasting can be enabled/disabled on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

3.5 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 (see *IP Policy Routing*) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

3.6 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

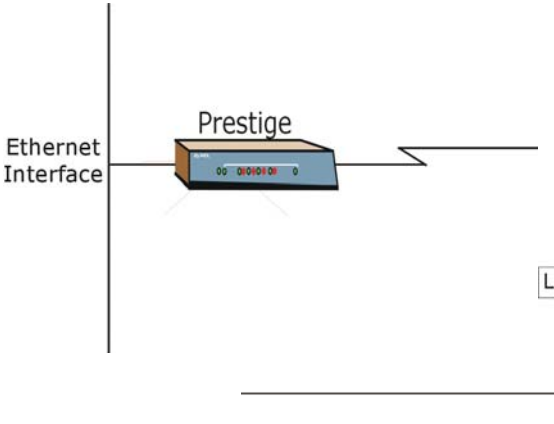

Figure 3-2 Physical Network

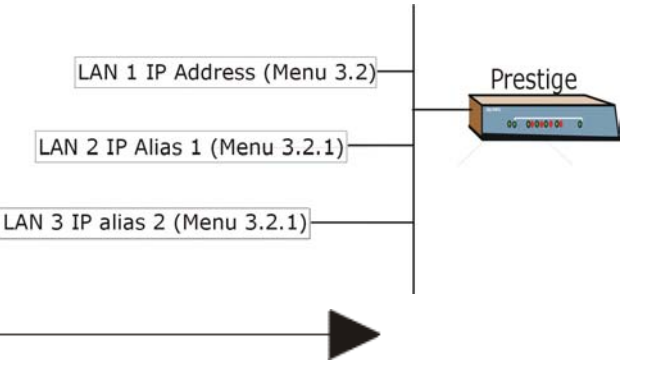

Figure 3-3 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your Prestige.

3.6.1 IP Alias Setup

Use menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACEBAR] to choose **Yes** and press [ENTER] to configure the second and third network.

```
                Menu 3.2 - TCP/IP and DHCP Setup

                DHCP Setup:
                 DHCP= Server
                 Client IP Pool Starting Address= 192.168.1.33
                 Size of Client IP Pool= 6
                 Primary DNS Server= 0.0.0.0
                 Secondary DNS Server= 0.0.0.0
                 Remote DHCP Server= N/A
                TCP/IP Setup:
                  IP Address= 192.168.1.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= None
                    Version= N/A
                  Multicast= None
                  IP Policies=
                  Edit IP Alias= No

                Press ENTER  to confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 3-4 Menu 3.2 — TCP/IP and DHCP Setup

Pressing [ENTER] displays **Menu 3.2.1 — IP Alias Setup**, as shown next.

```
                        Menu 3.2.1 - IP Alias Setup

                    IP Alias 1= No
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      RIP Direction= N/A
                      Version= N/A
                      Incoming protocol filters= N/A
                      Outgoing protocol filters= N/A
                    IP Alias 2= No
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      RIP Direction= N/A
                      Version= N/A
                      Incoming protocol filters= N/A
                      Outgoing protocol filters= N/A

                     Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 3-5 Menu 3.2.1 — IP Alias Setup

Follow the instructions in the following table to configure IP Alias parameters.

Table 3-1 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose **Yes** to configure the LAN network for the Prestige.	**Yes**
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.2.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **None**, **Both**, **In Only** or **Out Only**.	**None**
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

3.7 Route IP Setup

The first step is to enable the IP routing in **Menu 1 — General Setup**.

To edit menu 1, type in 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

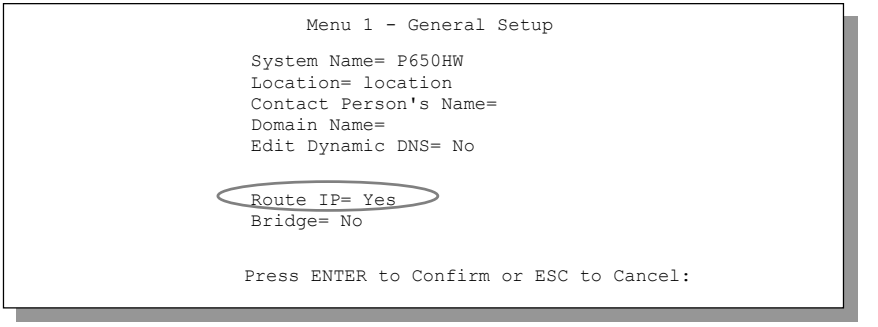

Figure 3-6 Menu 1 — General Setup

3.8 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your Prestige for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 — Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next:

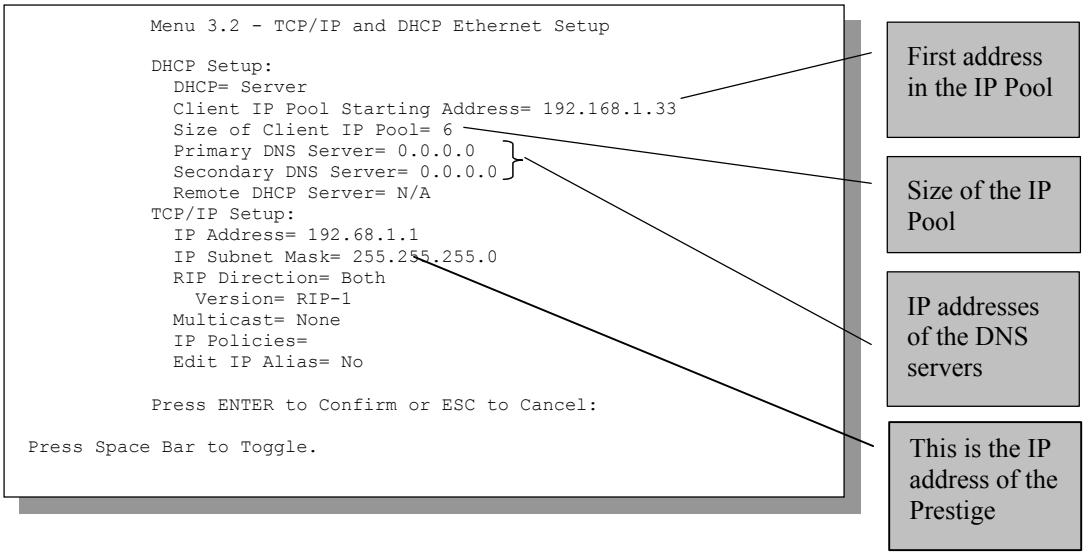
Menu 3.2 - TCP/IP and DHCP Ethernet Setup
DHCP Setup:
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 6
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.68.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-1
Multicast= None
IP Policies=
Edit IP Alias= No
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
First address in the IP Pool
Size of the IP Pool
IP addresses of the DNS servers
This is the IP address of the Prestige

Figure 3-7 Menu 3.2 — TCP/IP and DHCP Ethernet Setup

Follow the instructions in the following table on how to configure the DHCP fields.

Table 3-2 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup		
DHCP	If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case. When DHCP is used, the following items need to be set:	**Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and	

Table 3-2 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.	

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 3-3 TCP/IP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.	**None** (default)
IP Policies	Create policies using SMT menu 25 (see the *IP Policy Routing chapter*) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	2,4,7,9
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change **No** to **Yes** and press [ENTER] to for menu 3.2.1	**No** (default)

FIELD	DESCRIPTION	EXAMPLE
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

3.9 Wireless LAN

Your P650HW comes with a PCMCIA wireless card slot for 802.11b wireless LAN connectivity. With the wireless LAN feature you can configure your P650HW that allows wireless clients to communicate with any computer on your wired Ethernet network or to connect to the Internet via ADSL.

3.9.1 Wireless LAN Parameters

Channel

You can choose the radio channels depending on your geographical area.

ESS ID

Wireless LANs can be as simple as two computers with wireless network interface cards (NICs) communicating in a peer-to-peer network or as complex as a number of computers with wireless NICs communicating through access points (APs), which bridge network traffic to the wired LAN. You can setup the P650HW as an AP in a peer-to-peer network.

Extended Service Set (ESS) is defined as one or more APs that connect to a specific wired Ethernet LAN and their associated wireless clients. The ESS ID is a unique ID given to the access point and the wireless clients that participate in the same wireless network. You can think the EES ID as being similar to a workgroup name in a Microsoft network.

RTS Threshold

The RTS Threshold prevents the hidden node problem. Hidden node problem occurs when two stations are within the range of the same access point, but are not within the range of each other. The following figure illustrates the hidden node problem. Both stations (STA) are within the range of the AP, however, they cannot hear each other. Therefore, they are considered as hidden nodes from each other. When a station starts data transmission with the access point, it might not know that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the AP. The collision will most certainly results in a loss of messages for both stations.

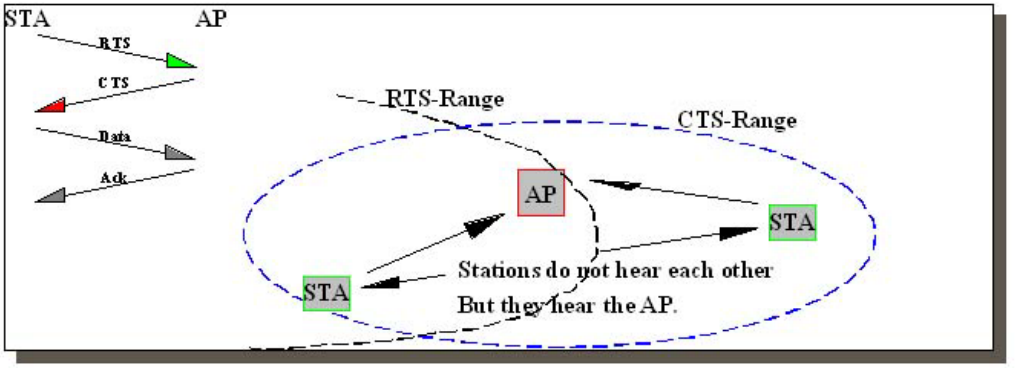

Figure 3-8 RTS Threshold

Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a possible hidden station, this station and its AP will use a Request to Send/Clear to Send protocol (RTS/CTS). The station will send an RTS message to the AP, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all stations within its range to notify all other stations to defer transmission. It will also confirm with the requesting station that the AP has reserved it for the time frame of the requested transmission.

The RTS function will be activated if the packet size exceeds the value you set. It is highly recommended that you set the value ranging from 0 to 2432.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

Fragmentation improves the efficiency when high traffic flows along in the wireless network.

WEP

The 11 Mbps wireless LAN provides powerful features such as WEP security. ZyXEL recommends that you change the ESSID setting of all devices on your network to a unique value, not the default value. A

further improvement in security can be obtained by using Wired Equivalent Privacy (WEP) data encryption. However, there may be a significant degradation of the data throughput on the wireless link when WEP is enabled.

3.9.2 Wireless LAN Setup

Use menu 3.5 to set up your P650HW as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

```
 Menu 3.5- Wireless LAN Setup

ESSID= Wireless
Hide ESSIS = No
Channel ID= CH01 2412MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= Disable
   Default Key= N/A
   Key1= N/A
   Key2= N/A
   Key3= N/A
   Key4= N/A
Edit MAC Address Filter= No

Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-9 Menu 3.5 - Wireless LAN Setup

The following table describes the fields in this screen.

Table 3-4 Wireless LAN Setup Field Description

FIELD	DESCRIPTION	EXMAPLE
ESSID	The ESSID (Extended Service Set IDentification) identifies the service set the wireless client is to connect to. Wireless clients associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless Service Set.	**Wireless**
Hide ESSID	Press [SPACE BAR] and select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning. Hiding the ESSID will also allow any wireless clients on the same channel to access the Prestige. Select **No** to allow any wireless client with the same ESSID and channel to access the Prestige.	**No**
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating	**CH01**

Table 3-4 Wireless LAN Setup Field Description

FIELD	DESCRIPTION	EXMAPLE
	frequency/channel depending on your particular region. Possible choices are **CH01 2412MHz**, **CH02 2417MHz**, **CH03 2422MHzCH11 2462MHz CH04 2427MHz**, **CH05 2432MHz**, **CH06 2437MHz**, **CH07 2442MHz**, **CH08 2447MHz**, **CH09 2452MHz**, **CH10 2457MHz or CH11 2462MHz**.	**2412MHz**
RTS Threshold	RTS(Request To Send) threshold (number of bytes) enables RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC Service Data Unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	**2432**
Fragment Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	**2432**
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **Disable** allows wireless clients to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to for the type of data encryption.	**Disable**
Default Key	Enter the number of the key as an active key.	
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers.	
Edit MAC Address Filter	To edit MAC address filtering table, press [SPACE BAR] to select **Yes** and press [ENTER] to open menu 3.5.1.	**No**
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

3.9.3 Wireless LAN MAC Address Filter

The next layer of security is MAC address filter. To allow a wireless client to associate with the Prestige, enter the MAC address of the wireless LAN card on that wireless client in the MAC address table

Figure 3-10

```
Menu 3.5.1 - WLAN MAC Address Filter

Active= No
Filter Action= Allowed Association
MAC Address Filter
  Address  1= 00:00:00:00:00:00
  Address  2= 00:00:00:00:00:00
  Address  3= 00:00:00:00:00:00
  Address  4= 00:00:00:00:00:00
  Address  5= 00:00:00:00:00:00
  Address  6= 00:00:00:00:00:00
  Address  7= 00:00:00:00:00:00
  Address  8= 00:00:00:00:00:00
  Address  9= 00:00:00:00:00:00
  Address 10= 00:00:00:00:00:00
  Address 11= 00:00:00:00:00:00
  Address 12= 00:00:00:00:00:00

Press ENTER to Confirm or ESC to Cancel:
```

Menu 3.5.1- WLAN MAC Address Filtering

Table 3-5 MAC Address Filter Field Description

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the Prestige, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, **Allowed Association**, permits association with the Prestige. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
Address 1..12	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the Prestige in these address fields.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

3.10 Internet Access Setup

3.11 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers supplied by your telephone company. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the Appendices for more information.

3.12 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

3.12.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

3.12.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

3.13 Encapsulation

Be sure to use the encapsulation method required by your ISP. The Prestige supports the following methods.

3.13.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment for instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Ethernet Encapsulation Gateway** field in menu 4 and in the **Rem IP Addr** field in menu 11.1. You can get this information from your ISP.

3.13.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to an xDSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the Appendices.

3.13.3 PPP

Please refer to RFC 2364 for more information on PPP over ATM Adaptation Layer 5 (AAL5). Refer to RFC 1661 for more information on PPP.

3.13.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

3.14 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP Address and ENET ENCAP Gateway.

3.14.1 Using PPP or PPPoE Encapsulation

If you have a dynamic IP, then the IP Address and ENET ENCAP Gateway fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the IP Address field and *not* the ENET ENCAP Gateway field.

3.14.2 Using RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the IP Address and ENET ENCAP Gateway fields as stated above.

3.14.3 Using ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the IP Address and ENET ENCAP Gateway fields as supplied by your ISP. However for a dynamic IP, the Prestige acts as a

DHCP client on the WAN port and so the IP Address and ENET ENCAP Gateway fields are not applicable (N/A) as they are assigned to the Prestige by the DHCP server.

3.15 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP and telephone company.

Use the following table to record your Internet Account Information. Note that if you are using PPP or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

Table 3-6 Internet Account Information

FIELD	DESCRIPTION	YOUR INFO
System Name	Name of the Prestige (optional).	
Service Name (PPPoE Encapsulation)	Enter the PPPoE service name if the ISP supplies one. Enter "any" if the ISP does not assign you one.	
Encapsulation	**PPPoE**, **RFC1483**, **PPP** or **ENET ENCAP**.	
Multiplexing	**LLC-based** or **VC-based**. If this information is not given, use the default.	
VPI	Enter your Virtual Path Identifier here.	
VCI	Enter your Virtual Channel Identifier here.	
My Login	Enter the login name assigned by your ISP (for PPP/PPPoE only).	
My Password	Enter the password associated with your ISP assigned **My Login** (for PPP/PPPoE only).	
Idle Timeout (PPPoE or PPP)	Enter the time lapse, in seconds, before you automatically disconnect from the PPPoE or PPP server.	
IP Address	Enter if your IP address is not dynamically assigned.	
Network Address Translation	**Full Feature**, **SUA Only** or **None**.	

Table 3-6 Internet Account Information

FIELD	DESCRIPTION	YOUR INFO
DNS Server Address Assignment	**Primary DNS server** **Secondary DNS server** Enter when using RFC 1483 Encapsulation or a static IP address.	
ENET ENCAP Gateway	**IP Address** **Gateway IP Address** Enter when using ENET ENCAP Encapsulation.	

3.15.1 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and "burstiness" or fluctuation of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

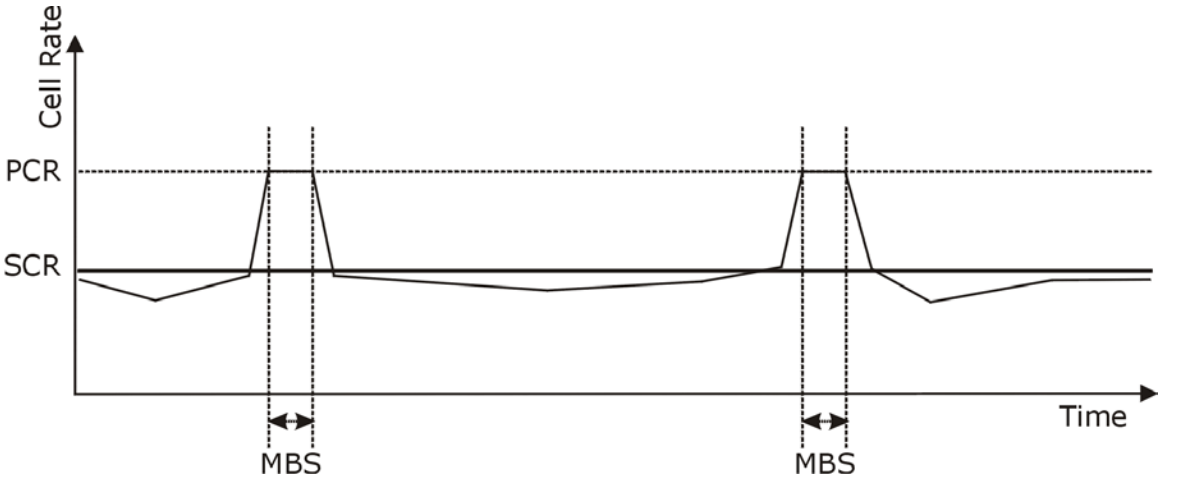

Figure 3-11 Example of Traffic Shaping

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**, as shown next.

```
                    Menu 4 - Internet Access Setup

                ISP's Name= MyISP
                Encapsulation= RFC 1483
                Multiplexing= VC-based
                VPI #= 8
                VCI #= 35
                ATM QoS Type= CBR
                  Peak Cell Rate (PCR)= 0
                  Sustain Cell Rate (SCR)= 0
                  Maximum Burst Size (MBS)= 0
                My Login= N/A
                My Password= N/A
                ENET ENCAP Gateway= N/A
                IP Address Assignment= Static
                  IP Address= 0.0.0.0
                Network Address Translation= SUA Only
                  Address Mapping Set= N/A

                Press ENTER to Confirm or ESC to Cancel:

            Press ENTER to confirm or ESC to cancel:
```

Figure 3-12 Internet Access Setup

The following table contains instructions on how to configure your Prestige for Internet access.

Table 3-7 Internet Access Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	MyISP
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPP**, **RFC 1483** or **ENET ENCAP**.	**RFC 1483**
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**.	**VC-based**
VPI #	Enter the Virtual Path Identifier (VPI) that the telephone company gives you.	8
VCI #	Enter the Virtual Channel Identifier (VCI) that the telephone company gives you.	35
ATM QoS Type	Press [SPACE BAR] and select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail.	**UBR**
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.	0
Sustain Cell Rate (SCR)= 0	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. Type the SCR; it must be less than the PCR.	0
Maximum Burst Size (MBS)= 0	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.	0
My Login	Configure the **My Login** and **My Password** fields for PPP and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation**,** then this field must be of the form user@domain where domain identifies your PPPoE service name.	N/A
My Password	Enter the password associated with the login name above.	N/A
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using **ENET ENCAP** encapsulation.	N/A
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	100 (Default)

Table 3-7 Internet Access Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] to select **Static** or **Dynamic** address assignment.	**Static**
IP Address	Enter the IP address supplied by your ISP if applicable.	0.0.0.0
Network Address Translation	Press [SPACE BAR] to select **None**, **SUA Only** or **Full Feature**. Please see the *NAT Chapter* for more details on the SUA (Single User Account) feature.	**SUA Only**
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See the *NAT* chapter for details.	**N/A**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

If all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

Part II:

ADVANCED APPLICATIONS

This part shows how to configure Remote Node, Remote Node TCP/IP and NAT.

Chapter 4
Remote Node Configuration

This chapter covers the parameters that are protocol-independent. Protocol-dependent configuration (TCP/IP and Bridging) is covered in the following chapters.

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

4.1 Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

Step 1. From the main menu, enter 11 to display **Menu 11 - Remote Node Setup.**

Step 2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

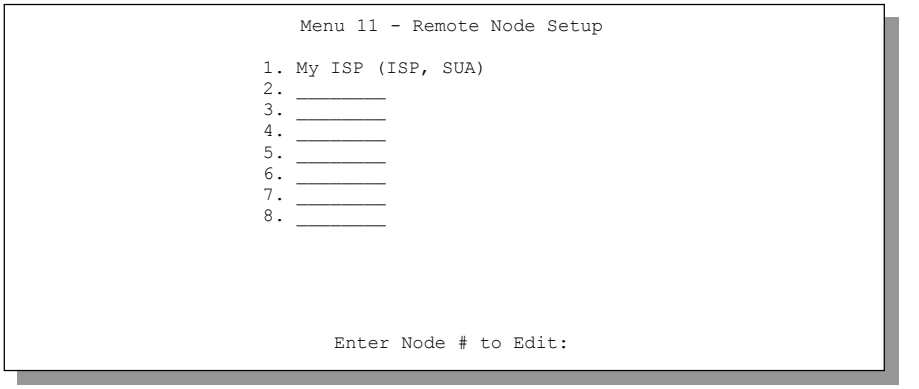

Figure 4-1 Menu 11 — Remote Node Setup

4.1.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. For LAN-to-LAN applications, for example, between a branch office and corporate headquarters, prior agreement on methods is necessary because encapsulation and multiplexing cannot be automatically determined. What method(s) you use depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

Scenario 1. One VC, Multiple Protocols

PPP (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

Scenario 2. One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPP** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

Scenario 3. Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Prestige does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Prestige will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name= myISP              Route= IP
Active= Yes                       Bridge= No

Encapsulation= PPP                Edit IP/Bridge= No
Multiplexing= LLC-based           Edit ATM Options= No
Service Name= N/A
Incoming:                         Telco Option:
  Rem Login=                        Allocated Budget(min)= 0
  Rem Password= ********            Period (hr)= 0
Outgoing:                           Schedule Sets= N/A
  My Login=                         Nailed-Up Connection= N/A
  My Password= ********           Session Options:
  Authen= CHAP/PAP                  Edit Filter Sets= No
                                    Idle Timeout (sec)= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

Figure 4-2 Menu 11.1 — Remote Node Profile

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 4-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	myISP
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or **No** to deactivate this node. Inactive nodes are displayed with a minus sign "–" in SMT menu 11.	**Yes**
Encapsulation	**PPP** refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) of **ENET ENCAP** are selected, then the **Rem Login**, **Rem Password**, **My Login**, **My Password**, **Edit PPP** Options and **Authen** fields are not applicable (**N/A**).	**PPP**
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either **VC-based** or **LLC-based**.	**LLC-based**
Service Name	When using **PPPoE** encapsulation, type the name of your PPPoE service here.	N/A

Table 4-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Incoming: Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the **Rem Password** will be used to authenticate this node.	
Rem Password	Type the password used when this remote node calls your Prestige.	
Outgoing: My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.	
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** – Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** – accept **CHAP** (Challenge Handshake Authentication Protocol) only. **PAP** – accept PAP (Password Authentication Protocol) only.	**PAP**
Route	This field determines the protocol used in routing. Options are **IP** and **None.**	**IP**
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select **Yes** to enable and **No** to disable.	**No**
Edit IP/Bridge	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.	**No**
Edit ATM Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.	**No**
Telco Option Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote	0 (default)

Table 4-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
	node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period (hr)** is 1 (hour).	(default)
Schedule Sets	This field is only applicable for **PPPoE** and **PPP** encapsulation. You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup* chapter.	
Nailed up Connection	This field is only applicable for **PPPoE** and **PPP** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options Edit Filter Sets	Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**No** (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.	0 (default)
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

4.1.3 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors' implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

4.2 Remote Node Setup

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

Step 1. In menu 11.1, make sure **IP** is among the protocols in the **Route** field.

Step 2. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.3** – **Remote Node Network Layer Options.**

```
                Menu 11.3 - Remote Node Network Layer Options

   IP Options:                          Bridge Options:
      IP Address Assignment= Static      Ethernet Addr Timeout (min)= 0
      Rem IP Addr: 0.0.0.0
      Rem Subnet Mask= 0.0.0.0
      My WAN Addr= 0.0.0.0
      NAT= Full Feature
        Address Mapping Set= 2
      Metric= 2
      Private= No
      RIP Direction= None
         Version= None
      Multicast= None
      IP Policies= 3,4,5,6

Press ENTER to Confirm or ESC to Cancel:
     Rem Node Name= myISP             Route= IP
```

Figure 4-3 Remote Node Network Layer Options

The next table explains fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 4-2 Remote Node Network Layer Options

FIELD	DESCRIPTITON	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to **Static**.	**Static**
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	

Table 4-2 Remote Node Network Layer Options

FIELD	DESCRIPTITON	EXAMPLE
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: Refers to local Prestige address, not the remote router address.	
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. Select **SUA Only** if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see section *7.3.1*). Select **None** to disable NAT.	**Full Feature**
Address Mapping Set	When **Full Feature** is selected in the **NAT** field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see the *NAT* chapter for details) and type that number here. When **SUA Only** is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see the *NAT* chapter for details).	2
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.	**None**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.	**None**
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see the *IP Policy Routing* chapter) and then apply them here.	3, 4, 5, 6

Table 4-2 Remote Node Network Layer Options

FIELD	DESCRIPTITON	EXAMPLE
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

4.3 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets (call protocol filter = 1). Include this in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

```
                    Menu 11.5 - Remote Node Filter

                         Input Filter Sets:
                           protocol filters= 11, 12
                             device filters=
                         Output Filter Sets:
                           protocol filters=
                             device filters=


          Enter here to CONFIRM or ESC to CANCEL:
```

Figure 4-4 Menu 11.5 — Remote Node Filter (RFC 1483 or ENET Encapsulation)

```
                    Menu 11.5 - Remote Node Filter

                         Input Filter Sets:
                           protocol filters= 11, 12
                             device filters=
                         Output Filter Sets:
                           protocol filters=
                             device filters=
                           Call Filter Sets:
                           Protocol filters=
                             Device filters=

          Enter here to CONFIRM or ESC to CANCEL:
```

Figure 4-5 Menu 11.5 — Remote Node Filter (PPP or PPPoE Encapsulation)

If you set the filters using the Internet Security in the Web Configurator, all your custom incoming protocol filters will be replaced by rule 11 and 12.

Chapter 5
Remote Node TCP/IP Configuration

This chapter shows a sample LAN-to-LAN application and how to configure TCP/IP remote node.

5.1 TCP/IP Configuration

The following sections describe how to configure the TCP/IP parameters of a remote node.

5.1.1 Editing TCP/IP Options

Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In menu 11.1, move the cursor to the **Edit ATM Options** field and then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of menu 11.6 for the Prestige, depending on whether you chose **VC-based/LLC-based** multiplexing and **PPP** encapsulation in menu 11.1.

VC-based Multiplexing

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. Separate VPI and VCI numbers must be specified for each protocol.

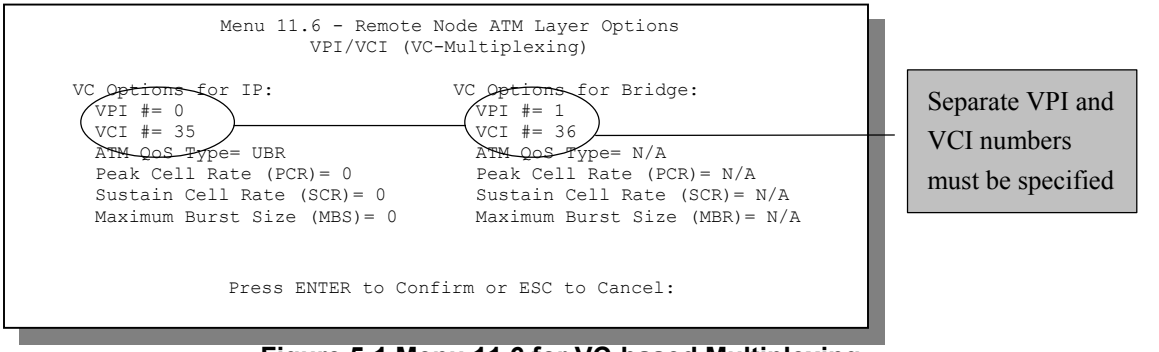
Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (VC-Multiplexing)
VC Options for IP:
VPI #= 0
VCI #= 35
ATM QoS Type= UBR
Peak Cell Rate (PCR)= 0
Sustain Cell Rate (SCR)= 0
Maximum Burst Size (MBS)= 0
VC Options for Bridge:
VPI #= 1
VCI #= 36
ATM QoS Type= N/A
Peak Cell Rate (PCR)= N/A
Sustain Cell Rate (SCR)= N/A
Maximum Burst Size (MBR)= N/A
Press ENTER to Confirm or ESC to Cancel:
Separate VPI and VCI numbers must be specified

Figure 5-1 Menu 11.6 for VC-based Multiplexing

LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

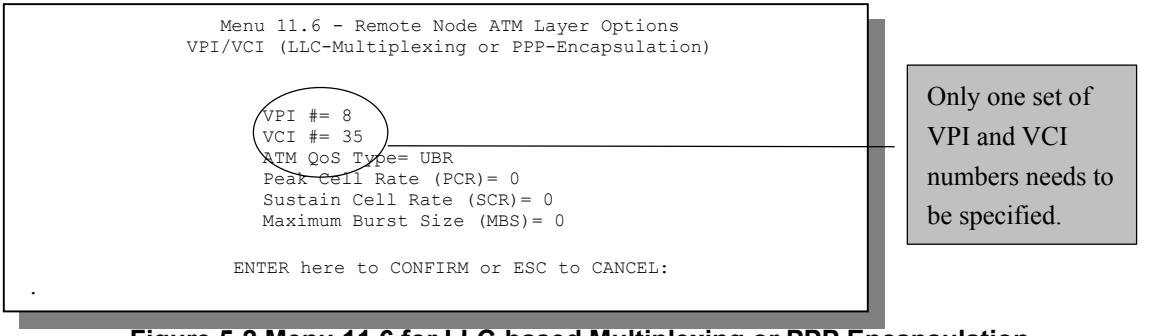
Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
Peak Cell Rate (PCR)= 0
Sustain Cell Rate (SCR)= 0
Maximum Burst Size (MBS)= 0
ENTER here to CONFIRM or ESC to CANCEL:
Only one set of VPI and VCI numbers needs to be specified.

Figure 5-2 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

The following figure uses sample IP addresses to help you understand the field of **My Wan Addr** in menu 11.3. Refer to the previous figure *LAN and WAN IPs* for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Addr** indicates the peer WAN IP.

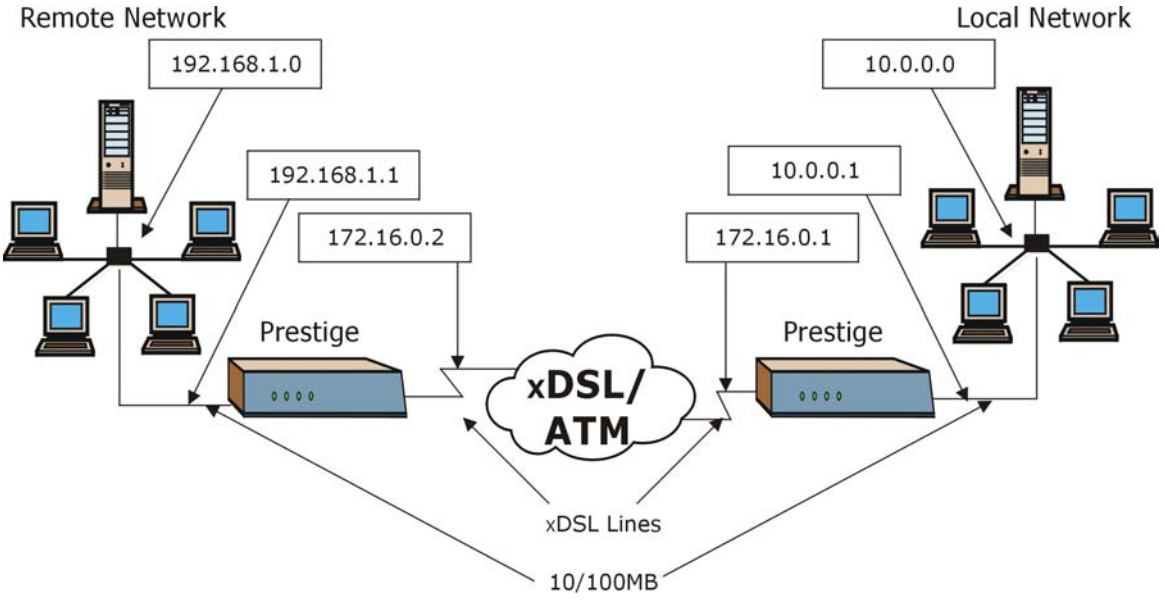

Figure 5-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure fields in **Menu 11.1 – Remote Node Profile**, as shown in the following table. For more details on the IP Option fields, refer to *Internet Access*.

Table 5-1 TCP/IP-Related Fields in Menu 11.1 — Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Route	Make sure **IP** is among the protocols in the **Route** field in **Menu 11.1 – Remote Node Profile**.	**IP**
Edit IP/Bridge	Press [SPACE BAR] to select **Yes** and press [ENTER] to display menu.	**Yes**

```
            Menu 11.3 - Remote Node Network Layer Options

IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set=2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

Figure 5-4 Remote Node Network Layer Options

The following table shows the fields in **Menu 11.3 — Remote Node Network Layer Options**.

Table 5-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (the first node); all other nodes are set to **Static**.	**Static**
Rem IP Addr	This is the IP address of the remote gateway**.** Type the remote Prestige's WAN IP address here (172.16.02 in the example *Figure 5-3* shown previously). If the remote Prestige's WAN IP address is 0.0.0.0, then type 192.168.1.1 (its LAN IP address) here.	0.0.0.0 (default)
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	0.0.0.0 (default)
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: Refers to local Prestige address, not the remote router address.	
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige.	**Full Feature**

Table 5-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	EXAMPLE
	Select **SUA Only** if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see section *7.3.1*). Select **None** to disable NAT.	
Address Mapping Set	When **Full Feature** is selected in the **NAT** field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see the *NAT* chapter for details) and type that number here. When **SUA Only** is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see the *NAT* chapter for details).	2
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**Yes**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.	**Both**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-2B**
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.	**IGMP-v2**
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas.	3, 4, 5, 6
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

5.1.2 IP Static Route Setup

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the Prestige about the networks beyond the remote nodes.

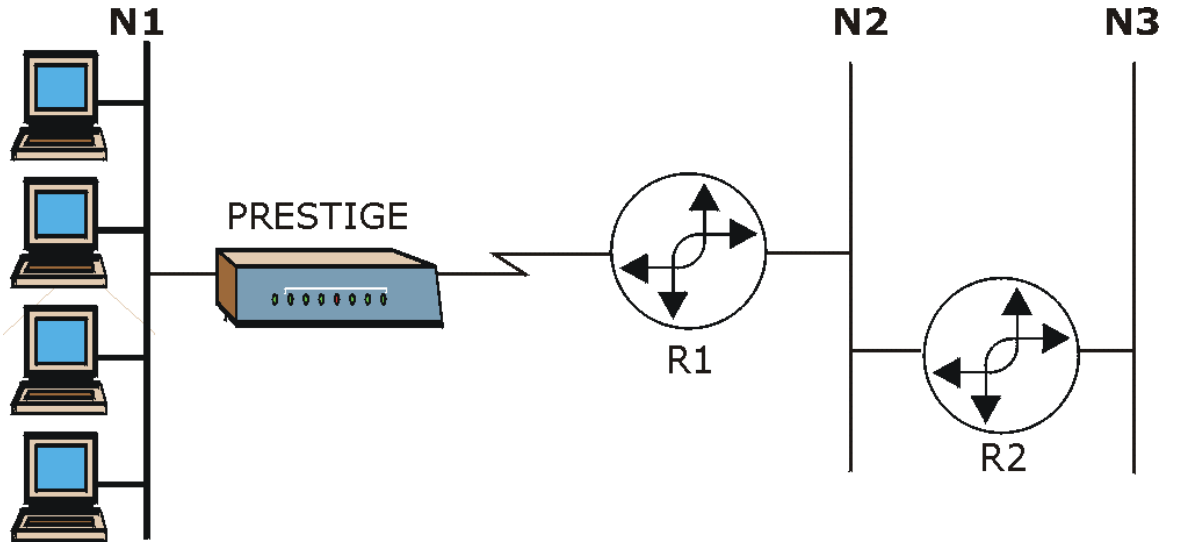

Figure 5-5 Sample Static Routing Topology

Configuration

Step 1. To configure an IP static route, use **Menu 12** – **Static Route Setup** (shown next).

```
Menu 12 - Static Route Setup

        1. IP Static Route
        3. Bridge Static Route


                Please enter selection:
```

Figure 5-6 Menu 12 — Static Route Setup

Step 2. From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).

```
                Menu 12.1 - IP Static Route Setup

                    1. ________
                    2. ________
                    3. ________
                    4. ________
                    5. ________
                    6. ________
                    7. ________
                    8. ________
                    9. ________
                    10. ________
                    11. ________
                    12. ________
                    13. ________
                    14. ________
                    15. ________
                    16. ________

                         Enter selection number:
```

Figure 5-7 Menu 12.1 — IP Static Route Setup

Step 3. Now, type the route number of a static route you want to configure.

```
              Menu 12.1.1 - Edit IP Static Route

                 Route #: 1
                 Route Name= ?
                 Active= No
                 Destination IP Address= ?
                 IP Subnet Mask= ?
                 Gateway IP Address= ?
                 Metric= 2
                 Private= No

          Press ENTER to Confirm or ESC to Cancel:
```

Figure 5-8 Edit IP Static Route

The following table describes the fields for **Menu 12.1.1 – Edit IP Static Route Setup**.

Table 5-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.

Table 5-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on *IP Subnet Mask* in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 6
Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

6.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

6.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

6.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:

Step 1. In menu 11.1, make sure the **Bridge** field is set to **Yes**.

Step 2. Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

```
                Menu 11.3 - Remote Node Network Layer Options

    IP Options:                          Bridge Options:
      IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
      Rem IP Addr: 0.0.0.0
      Rem Subnet Mask= 0.0.0.0
      My WAN Addr= 0.0.0.0
      NAT= Full Feature
        Address Mapping Set=2
      Metric= 2
      Private= No
      RIP Direction= Both
        Version= RIP-2B
      Multicast= IGMP-v2
      IP Policies=

  Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-1 Menu 11.3 — Remote Node Bridging Options

Table 6-1 Remote Node Bridge Options

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to **Yes**.
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select **Yes** and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

6.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1 (go to menu 12, choose option 3, then choose a static route to edit) as shown next.

```
                Menu 12.3.1 - Edit Bridge Static Route

                Route #: 1
                Route Name=
                Active= No
                Ether Address= ?
                IP Address=
                Gateway Node= 1



              Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-2 Menu 12.3.1 — Edit Bridge Static Route

The following table describes the **Edit Bridge Static Route** menu.

Table 6-2 Edit Bridge Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the route index number you typed in **Menu 12.3 – Bridge Static Route Setup**.
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active (**Yes**) or not (**No**).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 7
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

7.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

7.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Prestige, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 7-1 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside **host.**

7.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 7-2*), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

7.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Prestige keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

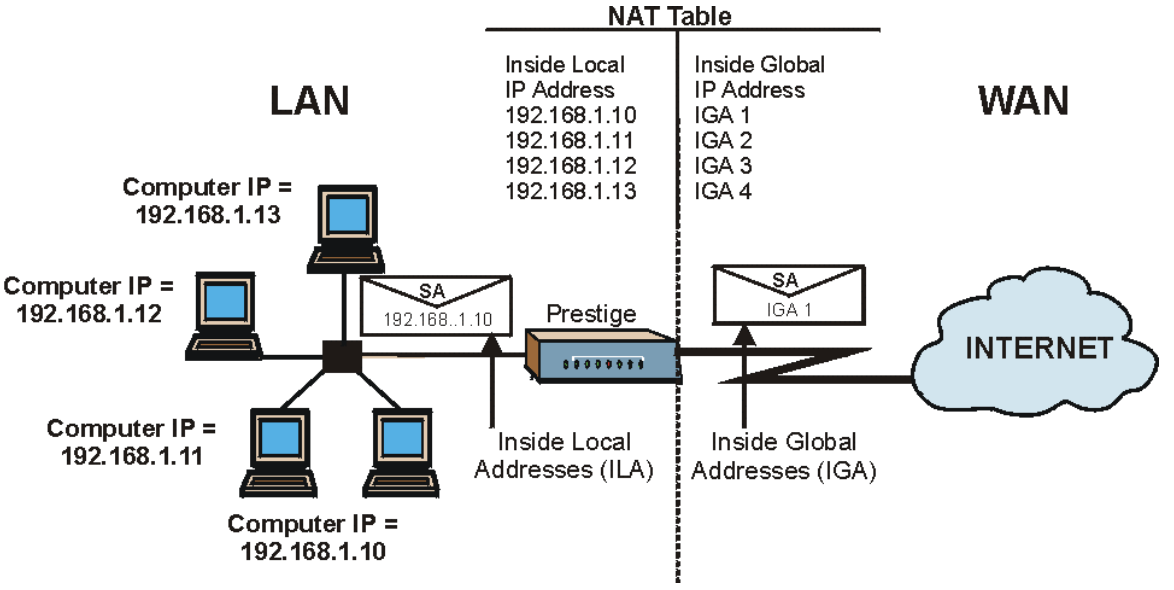

Figure 7-1 How NAT Works

7.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the Prestige can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

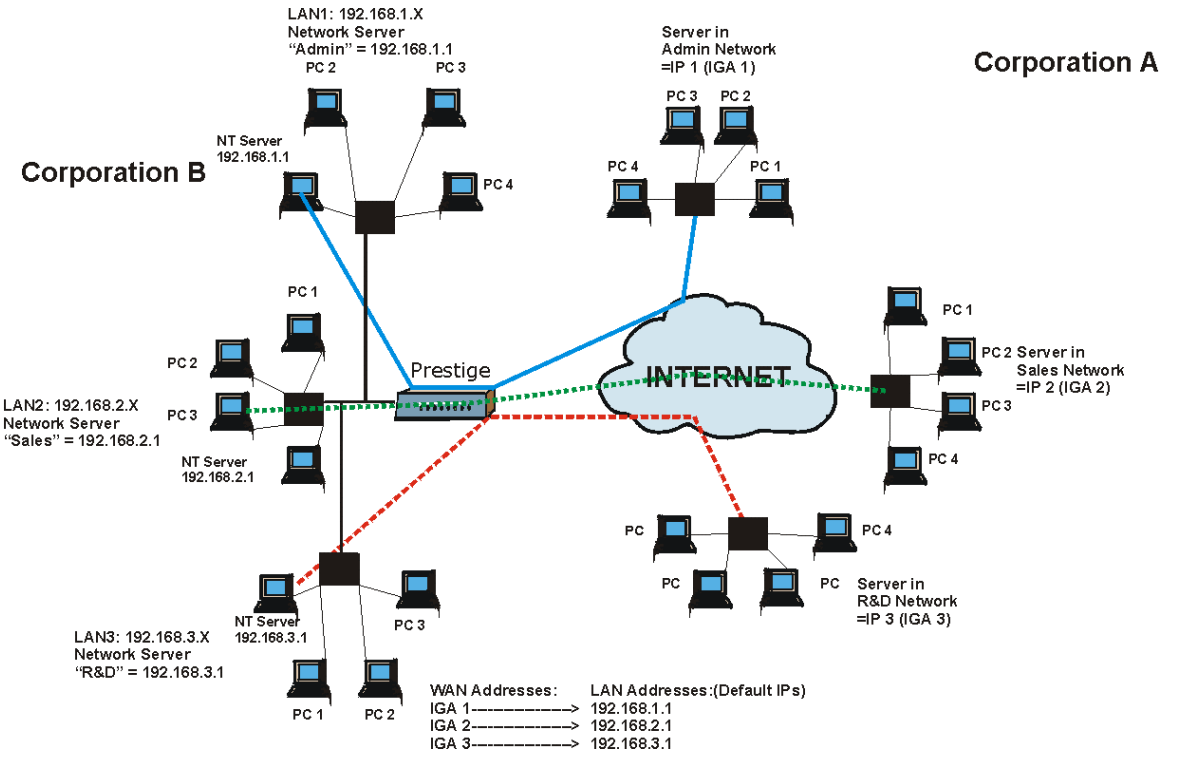

Figure 7-2 NAT Application With IP Alias

7.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

1. **One to One**: In One-to-One mode, the Prestige maps one local IP address to one global IP address.
2. **Many to One**: In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
3. **Many to Many Overload**: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.

4. **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the Prestige maps each local IP address to a unique global IP address.
5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

Port numbers do not **change for** One-to-One **and** Many-to-Many No Overload **NAT mapping types.**

The following table summarizes these types.

Table 7-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M:M No OV
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

7.2 Using NAT

7.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section *7.3.1* for a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 7-2*.

1. **Choose** SUA Only **if you have just one public WAN IP address for your Prestige.**

2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your Prestige.**

7.2.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

```
            Menu 4 - Internet Access Setup

                        ISP's Name= test
                        Encapsulation= RFC 1483
                        Multiplexing= LLC-based
                        VPI #= 1
                        VCI #= 1
                        Service Name= N/A
                        My Login= N/A
                        My Password= N/A
                        NAT= SUA Only
                          Address Mapping Set= N/A
                        IP Address Assignment= Static
                          IP Address= 0.0.0.0
                        ENET ENCAP Gateway= N/A


                        Press ENTER to Confirm or ESC to Cancel:

      Press Space Bar to Toggle.
```

Figure 7-3 Menu 4 — Applying NAT for Internet Access

The following figure shows how you apply NAT to the remote node in menu 11.1.

Step 1. Enter 11 from the main menu.

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

```
                    Menu 11.1 - Remote Node Profile

      Rem Node Name= test                  Route= IP+IPX
      Active= Yes                          Bridge= Yes

      Encapsulation= PPP                   Edit PPP Options= No
      Multiplexing= LLC-based              Rem IP Addr= 0.0.0.0
      Incoming:                            Edit IP/IPX/Bridge= Yes
        Rem Login=
        Rem Password= ********
      Outgoing:                            Session Options:
        My Login=                            Edit Filter Sets= No
        My Password= ********                PPPoE Idle Timeout(sec)= N/A
        Authen= CHAP/PAP                     PPPoE Service Name= N/A
                                             Schedule Sets= N/A



                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 7-4 Menu 11.3 — Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

Table 7-3 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION	EXAMPLE
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the **Address Mapping Set** field (menu 15.1 - see section *7.3.1*).	**Full Feature**
	Select **None** to disable NAT.	**None**
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see section *7.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.	**SUA Only**

7.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in Table 7-2. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the Prestige 10), a server rule must be set up inside the NAT Address Mapping set. Please see *section 7.4* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
                    Menu 15 — NAT Setup

          1.    Address Mapping Sets
          2.    NAT Server Sets


                Enter Menu Selection Number:
```

Figure 7-5 Menu 15 — NAT Setup

7.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

```
                    Menu 15.1 - Address Mapping Sets

                  1.
                  2.
                  3.
                  4.
                  5.
                  6.
                  7.
                  8.
                255. SUA (read only)


                       Enter Menu Selection Number:

Enter Menu Selection Number:
```

Figure 7-6 Menu 15.1 — Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 7.2.1)*. The fields in this menu cannot be changed.

```
                    Menu 15.1.255 - Address Mapping Rules

 Set Name=

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                    0.0.0.0                           Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-7 Menu 15.1.255 — SUA Address Mapping Rules

The following table explains the fields in this screen.

Menu 15.1.255 is read-only.

Table 7-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP Local End IP	**Local Start IP** is the starting local IP address (ILA) (see *Figure 7-1)*. **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	0.0.0.0 255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types discussed above (see *Table 7-2*). **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server

Table 7-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

```
                        Menu 15.1.1 - Address Mapping Rules

  Set Name= NAT_SET

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.
 2
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                  Action= Edit          Select Rule=

                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-8 Menu 15.1.1 — First Set

If the Set Name **field is left blank, the entire set will be deleted.**

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

Ordering Your Rules

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 7-5 Fields in Menu 15.1.1

FIELD	DESRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.	**Edit**
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An End IP address must be numerically greater than its corresponding IP Start address.

```
                Menu 15.1.1.1 Address Mapping Rule

          Type= One-to-One

          Local IP:
            Start=
            End  = N/A

          Global IP:
            Start=
            End  = N/A

          Server Mapping Set= N/A

               Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

Figure 7-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

Table 7-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Table 7-2. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 7.5.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0

Table 7-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.	
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

7.4 NAT Server Sets – Port Forwarding

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

The most often used port numbers are shown in the following table. Please refer to *RFC 1700* for further information about port numbers. Please also refer to the included disk for more examples and details on NAT.

Table 7-7 Services & Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

7.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

Step 2. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

```
                    Menu 15.2 - NAT Server Sets

                1. Server Set 1 (Used for SUA Only)
                2. Server Set 2
                3. Server Set 3
                4. Server Set 4
                5. Server Set 5
                6. Server Set 6
                7. Server Set 8
                8. Server Set 8
                9. Server Set 9
               10. Server Set 10




                        Enter Set Number to Edit:
```

Figure 7-10 Menu 15.2 — NAT Server Setup

Step 3. Enter 1 to go to **Menu 15.2.1 NAT Server Setup** as follows.

```
                  Menu 15.2.1 - NAT Server Setup

 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.    Default          Default        0.0.0.0
   2.      21               25           192.168.1.33
   3.      0                0            0.0.0.0
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      0                0            0.0.0.0

      Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-11 Menu 15.2.1 — NAT Server Setup

Step 4. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 5. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 6. Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

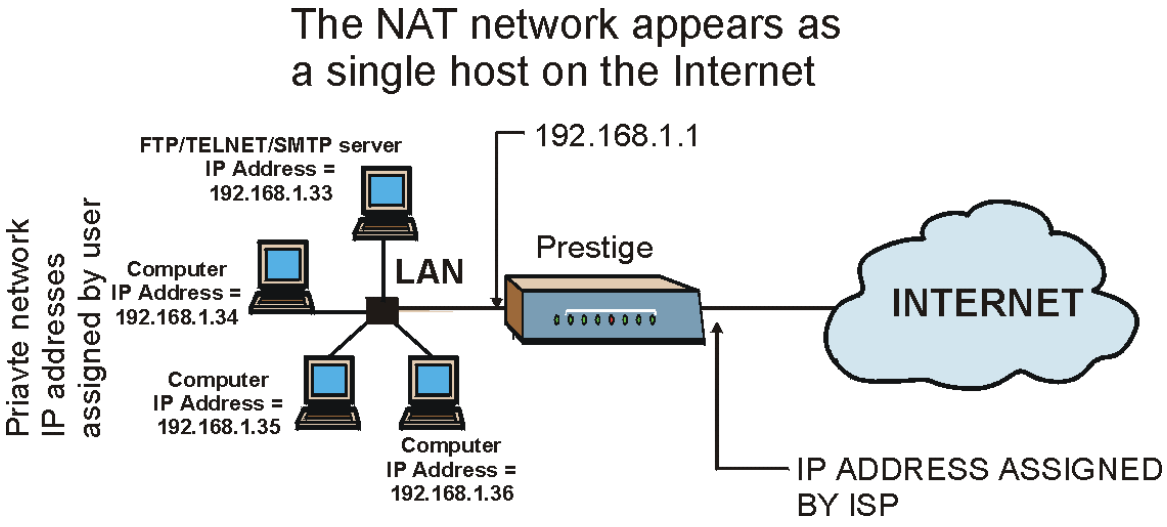

Figure 7-12 Multiple Servers Behind NAT Example

7.5 General NAT Examples

7.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

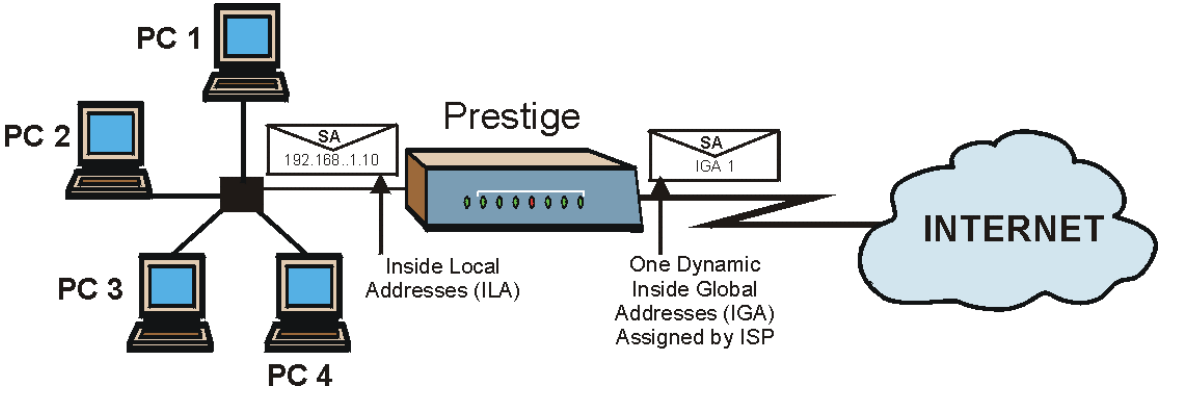

Figure 7-13 NAT Example 1

```
                Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= RFC-1483
Multiplexing= LLC-based
VPI #= 1
VCI #= 1
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 5500
  Sustained Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set=
```

Figure 7-14 Menu 4 — Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 7.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

7.5.2 Example 2: Internet Access with an Inside Server

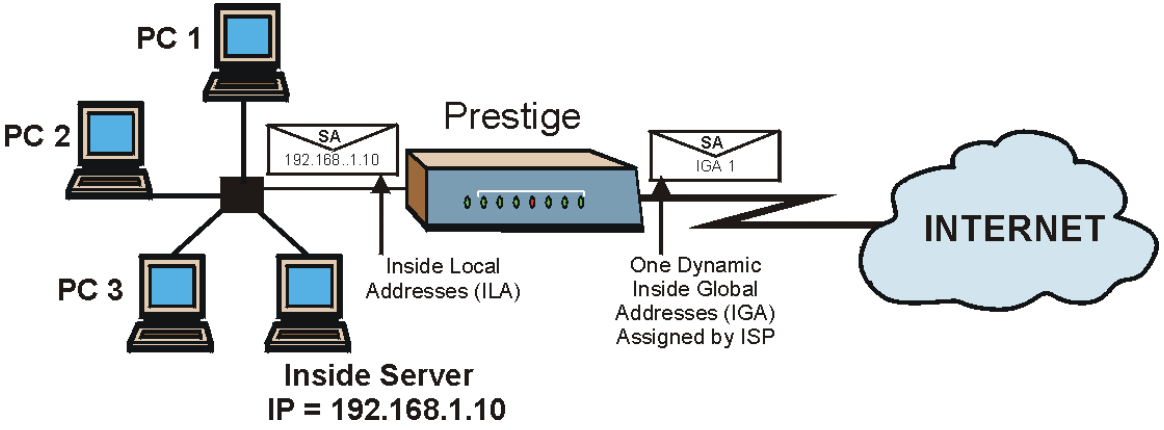

Figure 7-15 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

```
                Menu 15.2.1 - NAT Server Setup (Used for SUA Only)


Rule   Start Port No.   End Port No.   IP Address
-----------------------------------------------------
 1.      Default          Default        192.168.1.10
 2.        0                0             0.0.0.0
 3.        0                0             0.0.0.0
 4.        0                0             0.0.0.0
 5.        0                0             0.0.0.0
 6.        0                0             0.0.0.0
 7.        0                0             0.0.0.0
 8.        0                0             0.0.0.0
 9.        0                0             0.0.0.0
10.        0                0             0.0.0.0
11.        0                0             0.0.0.0
12.        0                0             0.0.0.0

     Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-16 Menu 15.2.1 — Specifying an Inside Server

7.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

Rule 1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

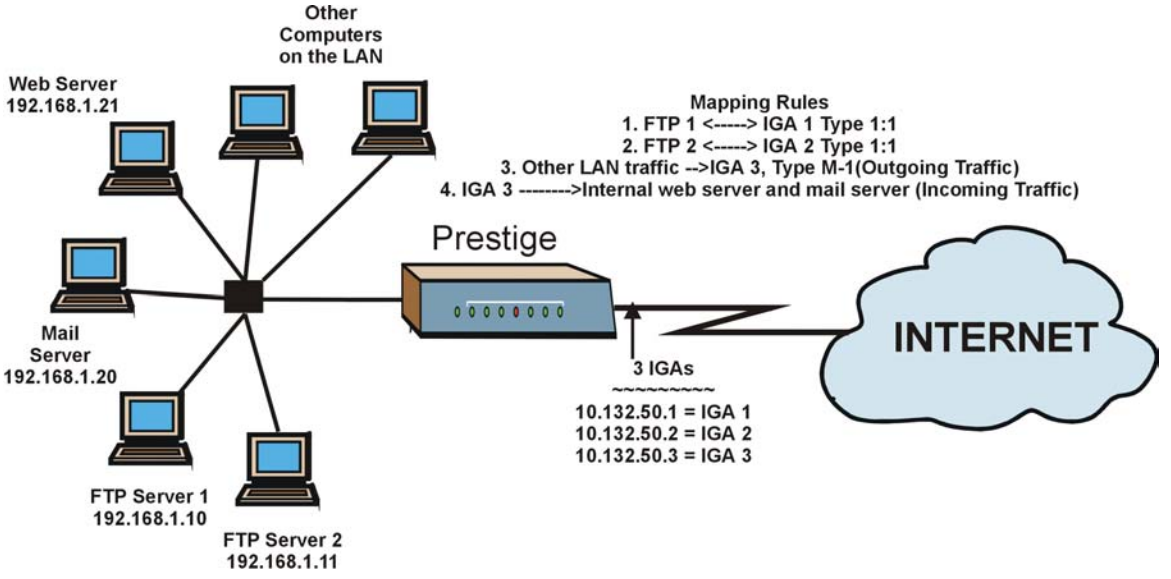

Figure 7-17 NAT Example 3

Step 1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in The following figure shows how to configure the first rule .

Step 2. Then enter 15 from the main menu.

Step 3. Enter 1 to configure the Address Mapping Sets.

Step 4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 7-19).*

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

Step 7. When finished, menu 15.1.1 should look like as shown in .

```
            Menu 11.3 - Remote Node Network Layer Options

IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

              Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-18 Example 3: Menu 11.3

The following figure shows how to configure the first rule

```
                Menu 15.1.1.1 Address Mapping Rule

          Type= One-to-One

          Local IP:
            Start= 192.168.1.10
            End  = N/A

          Global IP:
            Start= 10.132.50.1
            End  = N/A

          Server Mapping Set= N/A


                        Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

Figure 7-19 Example 3: Menu 15.1.1.1

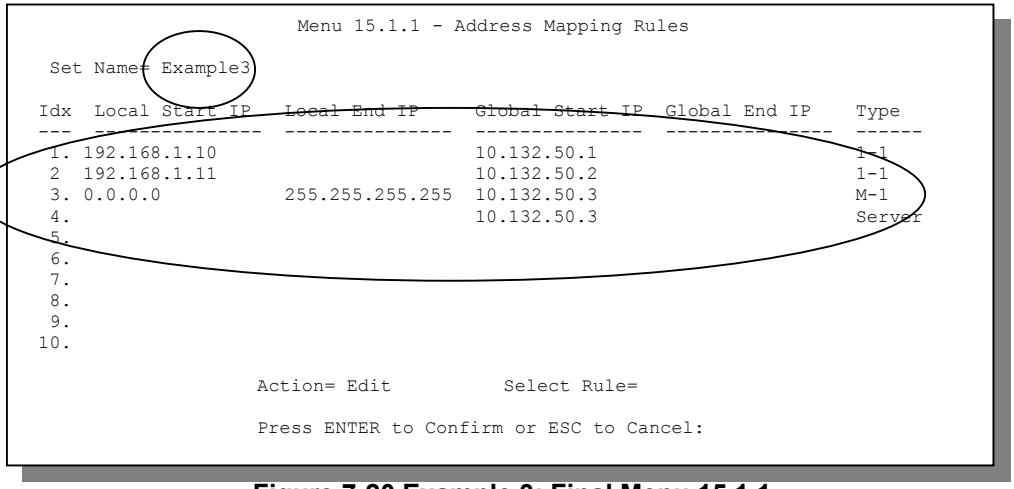

Figure 7-20 Example 3: Final Menu 15.1.1

Now configure the IGA3 to map to our web server and mail server on the LAN.

Step 8. Enter 15 from the main menu.

Step 9. Enter 2 in **Menu 15 - NAT Setup**.

Step 10. Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.

```
                    Menu 15.2.1 - NAT Server Setup

  Rule   Start Port No.   End Port No.   IP Address
 ------  --------------  -------------  ---------
    1.     Default          Default        0.0.0.0
    2.       80               80           192.168.1.21
    3.       25               25           192.168.1.20
    4.       0                0            0.0.0.0
    5.       0                0            0.0.0.0
    6.       0                0            0.0.0.0
    7.       0                0            0.0.0.0
    8.       0                0            0.0.0.0
    9.       0                0            0.0.0.0
   10.       0                0            0.0.0.0
   11.       0                0            0.0.0.0
   12.       0                0            0.0.0.0

          Press ENTER to Confirm or ESC to Cancel:
```

Example 3: Menu 15.2.1

7.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

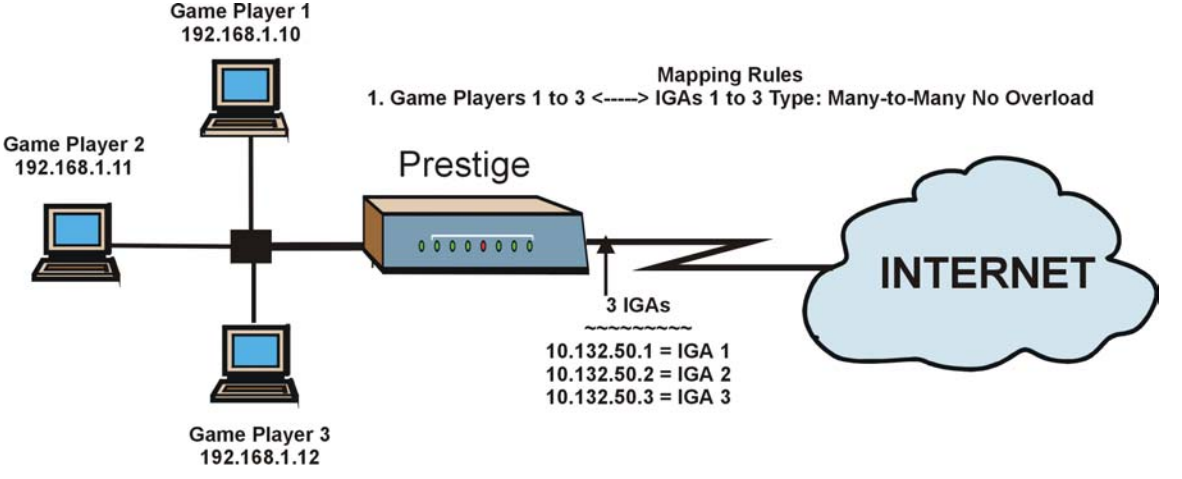

Figure 7-21 NAT Example 4

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One **and** Many-to-Many No Overload **mapping types.**

Follow the steps outlined in example 3 to configure these two menus as follows.

```
                    Menu 15.1.1.1 Address Mapping Rule

Type= Many-to-Many No Overload

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Server Mapping Set= N/A

                Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```
                        Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M:M NO OV
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                   Action= Edit          Select Rule=

                   Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-23 Example 4: Menu 15.1.1 — Address Mapping Rules

Part III:

ADVANCED MANAGEMENT

This part discusses Filtering, SNMP, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Information, IP Policy Routing, Call Scheduling and Remote Management.

Chapter 8
Filter Configuration

This chapter shows you how to create and apply filters.

8.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

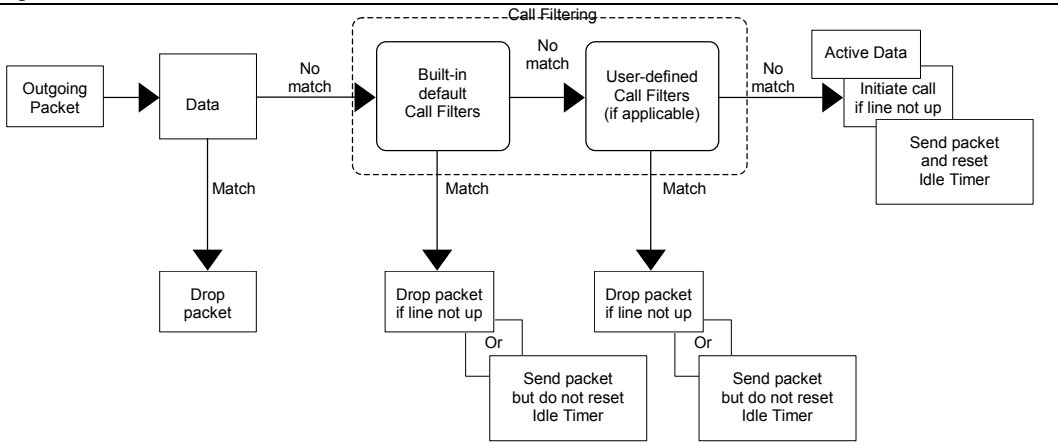

Figure 8-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

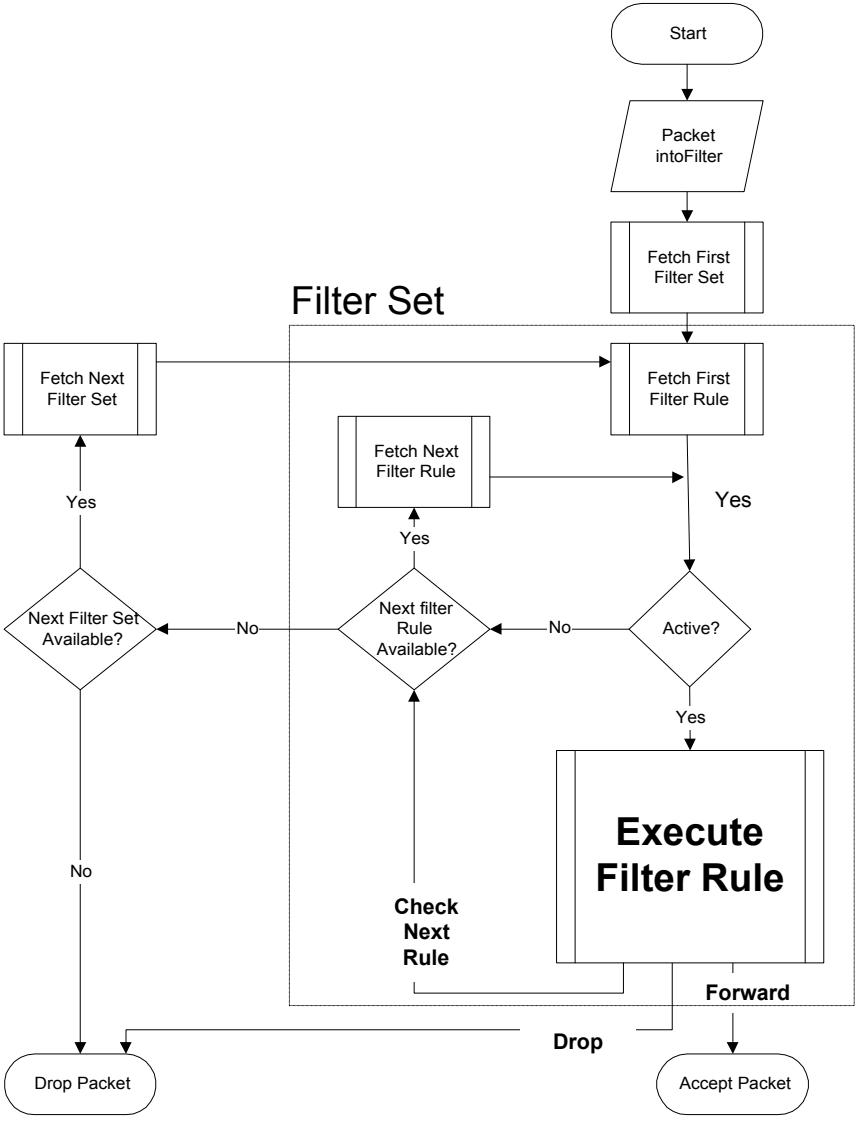

Figure 8-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your Prestige applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

8.2 Configuring a Filter Set

To configure a filter set, follow the steps shown next.

Step 1. Enter 21 in the main menu to display **Menu 21 – Filter Set Configuration**.

```
                Menu 21 - Filter Set Configuration

Filter                                  Filter
Set #        Comments                   Set #        Comments
------  -----------------              ------  -----------------
  1      NetBIOS_WAN                     7      _________________
  2      NetBIOS_LAN                     8      _________________
  3      TELNET_WAN                      9      _________________
  4      PPPoE                          10      _________________
  5      FTP_WAN                        11      _________________
  6                                     12      WebSet


               Enter Filter Set Number to Configure= 0

               Edit Comments= N/A

               Press ENTER to Confirm or ESC to Cancel:
```

Figure 8-3 Menu 21 — Filter Set Configuration

Step 2. Type the filter set to configure (no. 1 to 12) and press [ENTER].

Filter rule set 11 and 12 are used by the Web Configurator. Your custom configurator may be lost if you use rule 11 or 12.

Step 3. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message "Press [ENTER] to confirm…" to display **Menu 21.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21).

```
                    Menu 21.1 - Filter Rules Summary

# A Type                        Filter Rules                        M m n
 - - ---- ------------------------------------------- --------- - - -
   1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                    N D N
   2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                    N D N
   3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                    N D N
   4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                   N D N
   5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                   N D N
   6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                   N D F


Enter Filter Rule Number (1-6) to Configure: 1
```

Figure 8-4 NetBIOS_WAN Filter Rules Summary

```
                    Menu 21.2 - Filter Rules Summary

# A Type                        Filter Rules                        M m n
 - - ---- ------------------------------------------- --------- - - -
   1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53             N D F
   2 Y
   3 Y
   4 Y
   5 Y
   6 Y

Enter Filter Rule Number (1-6) to Configure: 1
```

Figure 8-5 NetBIOS_LAN Filter Rules Summary

```
                    Menu 21.3 - Filter Rules Summary

# A Type                       Filter Rules                            M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                          N D F
2 N
3 N
4 N
5 N
6 N

              Enter Filter Rule Number (1-6) to Configure:
```

Figure 8-6 Telnet_WAN Filter Rules Summary

```
                    Menu 21.4 - Filter Rules Summary

# A Type                       Filter Rules                            M m n
- - ---- ------------------------------------------------------------ - - -
1 Y Gen  Off=12, Len=2, Mask=ffff, Value=8863                          N F N
2 Y Gen  Off=12, Len=2, Mask=ffff, Value=8864                          N F D
3 N
4 N
5 N
6 N

                Enter Filter Rule Number (1-6) to Configure:
```

Figure 8-7 PPPoE Filter Rules Summary

```
                    Menu 21.5 - Filter Rules Summary

# A Type                       Filter Rules                          M m n
- - ----  ------------------------------------------------------------ - - -
1 Y IP    PR=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                         N D F
2 N
3 N
4 N
5 N
6 N


              Enter Filter Rule Number (1-6) to Configure:
```

Figure 8-8 FTP_WAN Filter Rules Summary

In filter rule 6, FTP_TELNET_WEB, the WEB means that HTTP and TFTP traffic are blocked.

```
                    Menu 21.12 - Filter Rules Summary

 # A Type                       Filter Rules                          M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                          N D N
 2 N IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                          N D N
 3 N IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                          N D N
 4 N IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=69                         N D F
 5 N
 6 N


              Enter Filter Rule Number (1-6) to Configure: 1
```

Figure 8-9 WebSet Filter Rules Summary

8.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1 and 21.2.

Table 8-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 8-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	
Off	Offset
Len	Length

8.3 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1 – Filter Rules Summary** and press [ENTER] to open menu 21.1.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

8.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1 – TCP/IP Filter Rule**, as shown next.

```
                    Menu 21.1.1 - TCP/IP Filter Rule
                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 6      IP Source Route= No
                Destination: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 137
                             Port # Comp= Equal
                     Source: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 0
                             Port # Comp= None
                TCP Estab= No
                More= No              Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 8-10 Menu 21.1.1 — TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 8-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	1,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.	**TCP/IP Filter Rule**
Active	Select **Yes** to activate or **No** to deactivate the filter rule.	**No** (default)
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of O matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	**No** (default)

Table 8-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	IP mask
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	**No** (default)
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**

Table 8-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

The following figure illustrates the logic flow of an IP filter.

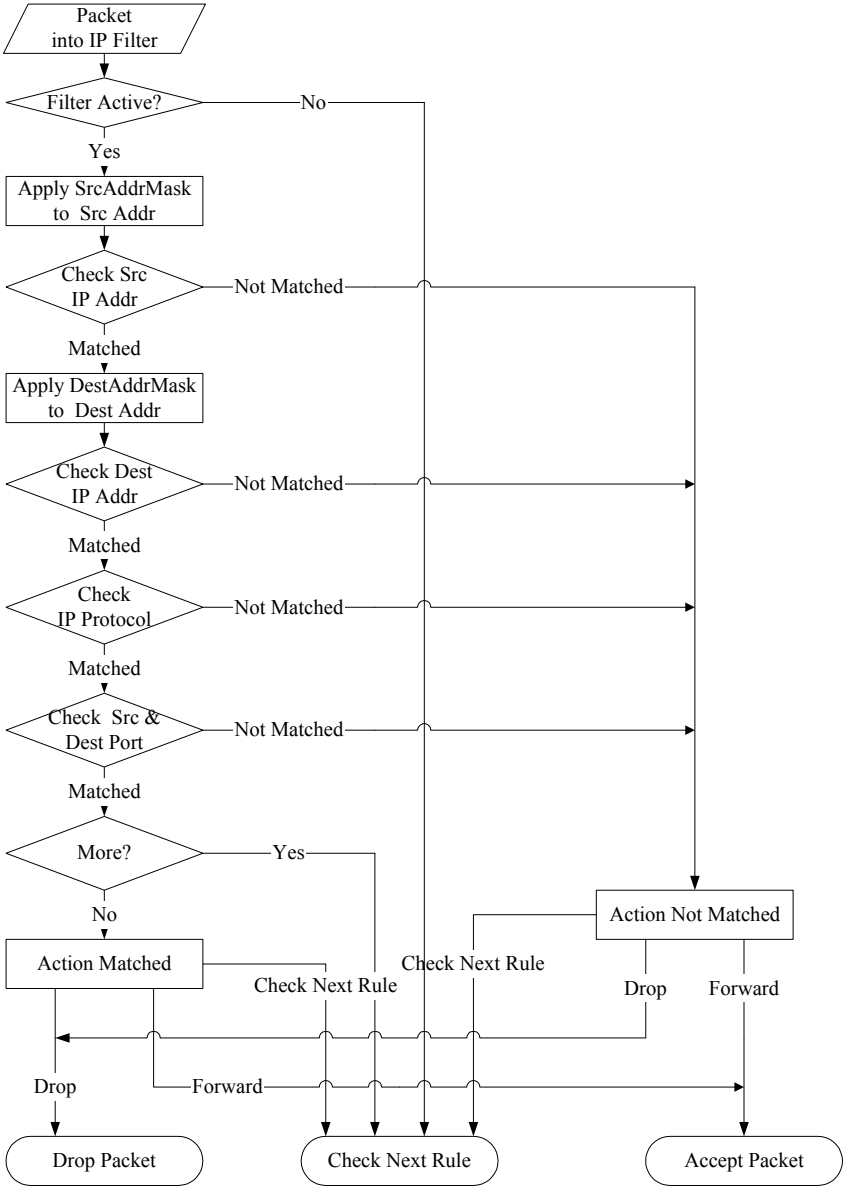

Figure 8-11 Executing an IP Filter

8.3.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for example 5. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.5.1 – Generic Filter Rule**, as shown in the following figure.

```
                    Menu 21.5.1 - Generic Filter Rule

                Filter #: 5,1
                Filter Type= Generic Filter Rule
                Active= No
                Offset= 0
                Length= 0
                Mask= N/A
                Value= N/A
                More= No            Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 8-12 Menu 21.5.1 — Generic Filter Rule

The next table describes the fields in the Generic Filter Rule menu.

Table 8-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	5,1
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**.	**Generic Filter Rule**
Active	Select **Yes** to turn on or **No** to turn off the filter rule.	**No** (default)
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

8.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

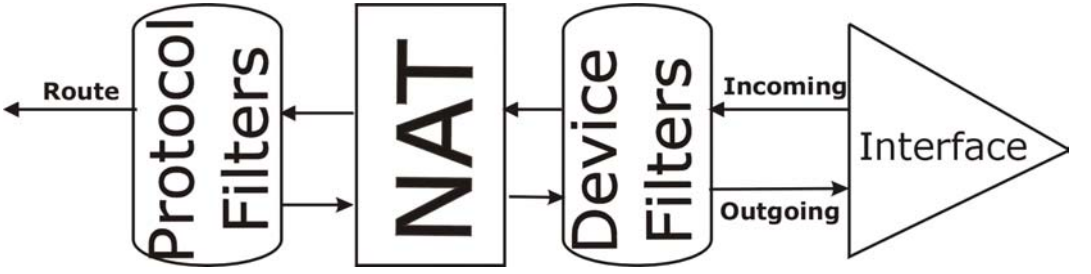

Figure 8-13 Protocol and Device Filter Sets

8.5 Example Filter

Let's look at an example to block outside users from telnetting into the Prestige. See the *included disk* for example filters.

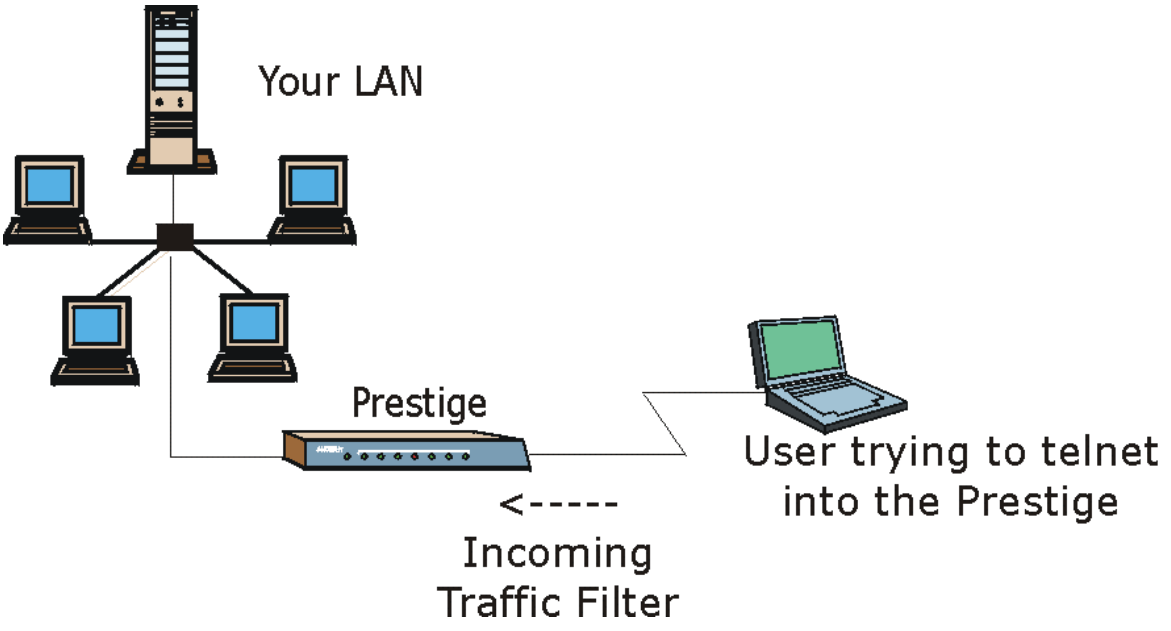

Figure 8-14 Sample Telnet Filter

Step 1. Enter 21 from the main menu to open **Menu 21 — Filter Set Configuration**.

Step 2. Enter the index number of the filter set you want to configure (in this case 3).

Step 3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].

Step 4. Press [ENTER] at the message "Press [ENTER] to confirm or [ESC] to cancel" to open **Menu 21.3.1 — TCP/IP Filter Rule**.

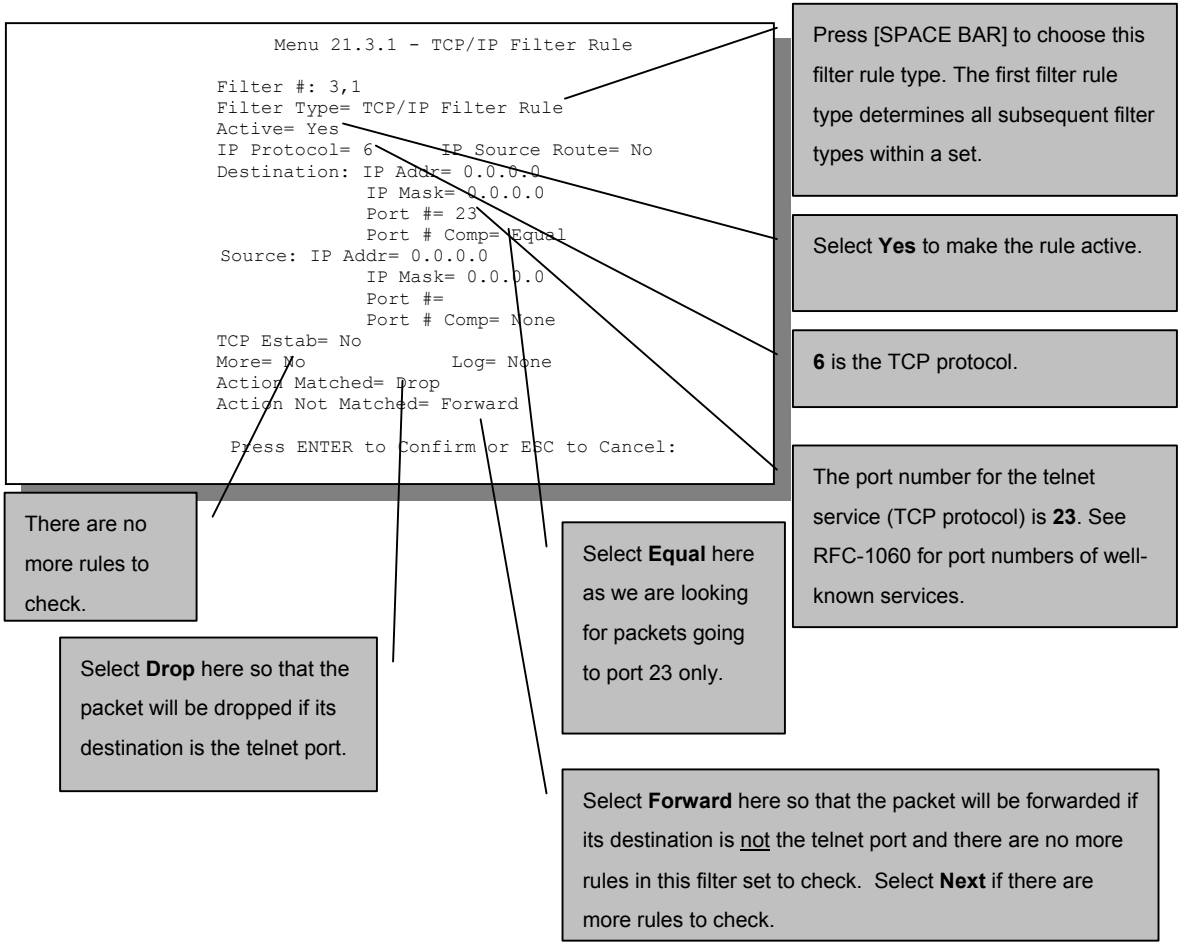
Menu 21.3.1 - TCP/IP Filter Rule
Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6 IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 23
Port # Comp= Equal
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #=
Port # Comp= None
TCP Estab= No
More= No Log= None
Action Matched= Drop
Action Not Matched= Forward
Press ENTER to Confirm or ESC to Cancel:
Press [SPACE BAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.
Select Yes to make the rule active.
6 is the TCP protocol.
The port number for the telnet service (TCP protocol) is 23. See RFC-1060 for port numbers of well-known services.
There are no more rules to check.
Select Equal here as we are looking for packets going to port 23 only.
Select Drop here so that the packet will be dropped if its destination is the telnet port.
Select Forward here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select Next if there are more rules to check.

Figure 8-15 Sample Filter — Menu 21.3.1

Step 5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

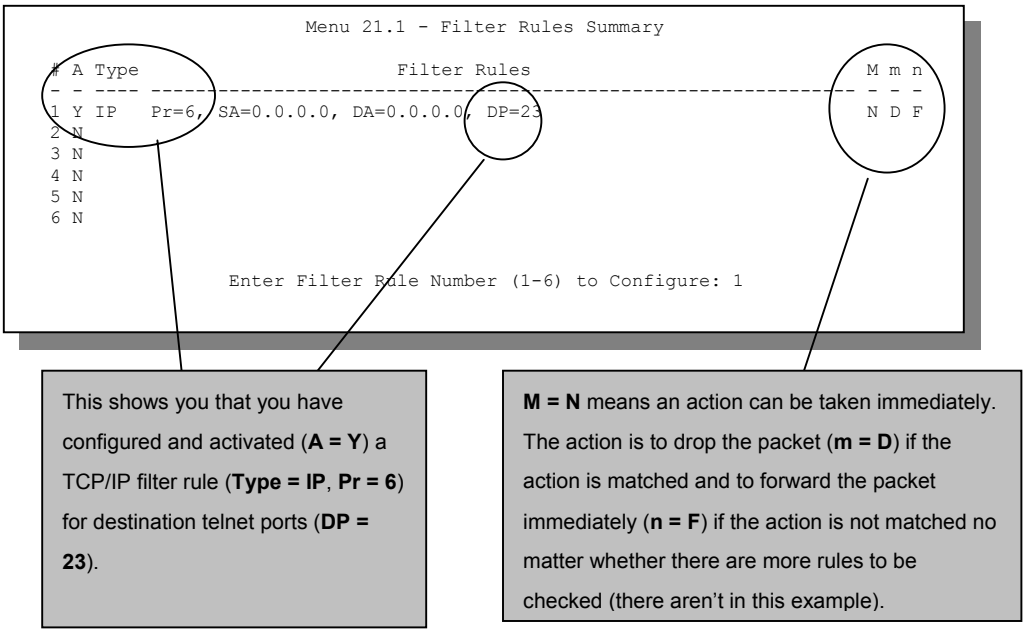
Menu 21.1 - Filter Rules Summary
A Type Filter Rules M m n
1 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23 N D F
2 N
3 N
4 N
5 N
6 N
Enter Filter Rule Number (1-6) to Configure: 1
This shows you that you have configured and activated (A = Y) a TCP/IP filter rule (Type = IP, Pr = 6) for destination telnet ports (DP = 23).
M = N means an action can be taken immediately. The action is to drop the packet (m = D) if the action is matched and to forward the packet immediately (n = F) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 8-16 Sample Filter Rules Summary — Menu 21.1

After you have created the filter set, you must apply it.

Step 1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

8.6 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 8-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

8.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

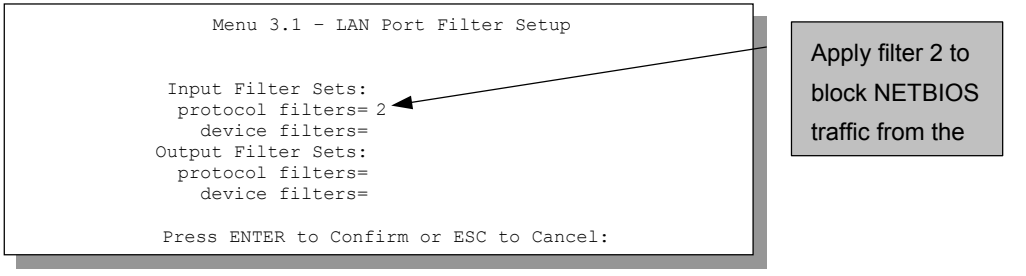
Menu 3.1 - LAN Port Filter Setup
Input Filter Sets:
protocol filters= 2
device filters=
Output Filter Sets:
protocol filters=
device filters=
Press ENTER to Confirm or ESC to Cancel:
Apply filter 2 to block NETBIOS traffic from the

Figure 8-17 Filtering Ethernet Traffic

8.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

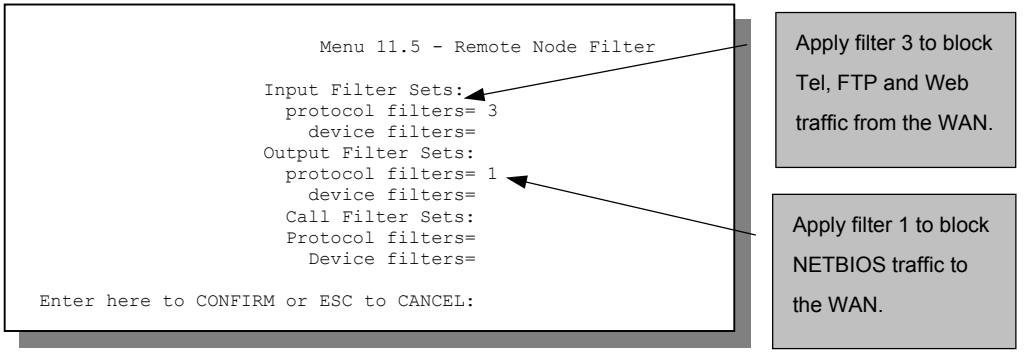
Menu 11.5 - Remote Node Filter
Input Filter Sets:
protocol filters= 3
device filters=
Output Filter Sets:
protocol filters= 1
device filters=
Call Filter Sets:
Protocol filters=
Device filters=
Enter here to CONFIRM or ESC to CANCEL:
Apply filter 3 to block Tel, FTP and Web traffic from the WAN.
Apply filter 1 to block NETBIOS traffic to the WAN.

Figure 8-18 Filtering Remote Node Traffic

Note that call filter sets are visible when you select PPP or PPPoE encapsulation.

Chapter 9
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

SNMP is only available if TCP/IP is configured.

9.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

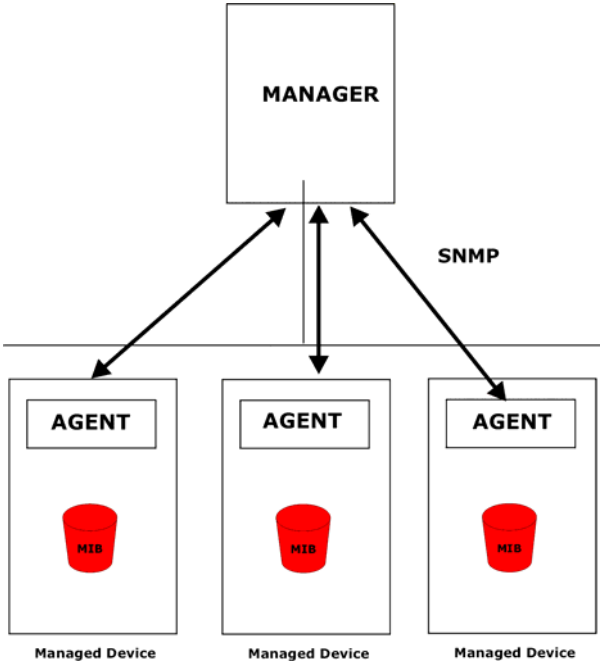

Figure 9-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the Prestige). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

9.2 Supported MIBs

The Prestige supports RFC-1215 and MIB II as defined in RFC-1213. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

9.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

```
                    Menu 22 - SNMP Configuration

                SNMP:
                  Get Community= public
                  Set Community= public
                  Trusted Host= 0.0.0.0
                  Trap:
                    Community= public
                    Destination= 0.0.0.0


                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 9-2 Menu 22 — SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 9-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		public
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

9.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 9-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.
4	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Table 9-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	xDSL

Chapter 10
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

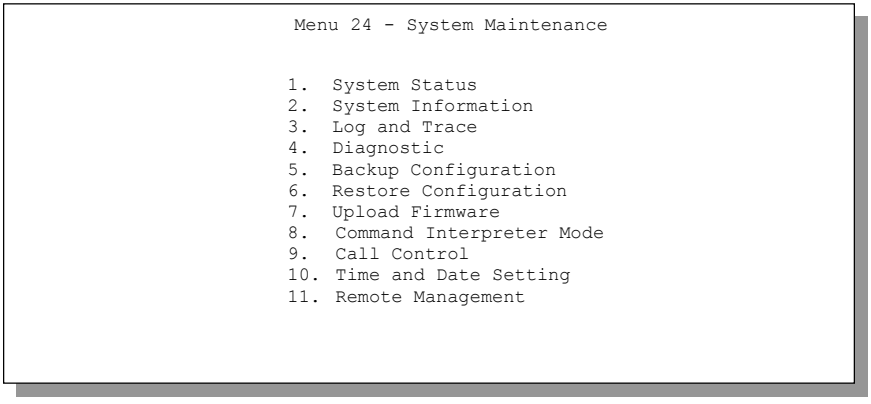

Figure 10-1 Menu 24 — System Maintenance

10.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

```
                        Menu 24.1 - System Maintenance - Status          hh:mm:ss
                                                                 Sat. Jan. 01, 2000

Node-Lnk    Status         TxPkts     RxPkts     Errors   Tx B/s   Rx B/s      Up Time
  1-ENET      Up              211          0          0        0        0      0:26:20
  2          N/A                0          0          0        0        0      0:00:00
  3          N/A                0          0          0        0        0      0:00:00
  4          N/A                0          0          0        0        0      0:00:00
  5          N/A                0          0          0        0        0      0:00:00
  6          N/A                0          0          0        0        0      0:00:00
  7          N/A                0          0          0        0        0      0:00:00
  8          N/A                0          0          0        0        0      0:00:00


My WAN IP (from ISP) :

   Ethernet:                                        WAN:
     Status: 10M/Half Duplex          Tx Pkts: 53      Line Status: Up
     Collisions: 0                    Rx Pkts: 36      Upstream Speed:     0 Kbps
   CPU Load= 3.8%                                      Downstream Speed:     0 Kbps



                                  Press Command:
                        COMMANDS: 1-Reset Counters   ESC-Exit
```

Figure 10-2 Menu 24.1 — System Maintenance — Status

The following table describes the fields present in **Menu 24.1** — **System Maintenance** — **Status**.

Table 10-1 System Maintenance — Status Menu Fields

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type. Link types are: PPP, ENET, 1483.
Status	Shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the current remote node.
My WAN IP (from ISP)	The IP address of the ISP remote node.
Ethernet	Shows statistics for the LAN.

Table 10-1 System Maintenance — Status Menu Fields

FIELD	DESCRIPTION
Status	Shows the current status of the LAN.
Tx Pkts	The number of transmitted packets to the LAN.
Rx Pkts	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	Shows statistics for the WAN.
Line Status	Shows the current status of the xDSL line which can be Up or Down.
Upstream Speed	Shows the upstream transfer rate in kbps.
Downstream Speed	Shows the downstream transfer rate in kbps.
CPU Load	Specifies the percentage of CPU utilization.

10.2 System Information

To get to the System Information:

Step 1. Enter 24 to display **Menu 24** — **System Maintenance**.

Step 2. Enter 2 to display **Menu 24.2** — **System Information**.

Step 3. From this menu you have two choices as shown in the next figure:

```
Menu 24.2 - System Information
      1. System Information
      2. Console Port Speed



            Please enter selection:
```

Figure 10-3 Menu 24.2 — System Information and Console Port Speed

Console port speed is included here for use by experienced technicians only.

10.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

```
Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS F/W Version: V3.40(ES.0)b8 | 11/20/2001
ADSL Chipset Vendor: Alcatel, Version  3.8.130
Standard: Multi-Mode

LAN
  Ethernet Address: 00:a0:c5:01:23:45
  IP Address: 192.168.1.1
  IP Mask: 255.255.255.0
  DHCP: Server

       Press ESC or RETURN to Exit:
```

Figure 10-4 Menu 24.2.1 — System Maintenance — Information

Table 10-2 Fields in System Maintenance

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
ADSL Chipset Vendor	**Displays the vendor of the ADSL chipset and DSL version.**
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.

Table 10-2 Fields in System Maintenance

FIELD	DESCRIPTION
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

10.3 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

10.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

Step 1. Type 24 in the main menu to display **Menu 24** – **System Maintenance**.

Step 2. From menu 24, type 3 to display **Menu 24.3** – **System Maintenance** – **Log and Trace**.

```
Menu 24.3 - System Maintenance - Log and Trace

    1. View Error Log
    2. UNIX Syslog



Please enter selection
```

Figure 10-5 Menu 24.3 — System Maintenance — Log and Trace

Step 3. Enter 1 from **Menu 24.3** — **System Maintenance** — **Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
  59 Thu Jan 01 00:00:03 1970 PP0f  INFO  LAN promiscuous mode <0>
  60 Thu Jan 01 00:00:03 1970 PP00 -WARN  SNMP TRAP 0: cold start
  61 Thu Jan 01 00:00:03 1970 PP00  INFO  main: init completed
  62 Thu Jan 01 00:00:19 1970 PP00  INFO  SMT Session Begin
  63 Thu Jan 01 00:00:24 1970 PP0a  WARN  MPOA Link Down
Clear Error Log (y/n):
```

Figure 10-6 Sample Error and Information Messages

10.3.2 Syslog and Accounting

The Prestige uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance — UNIX Syslog**, as shown next.

```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

                       UNIX Syslog:
                         Active= No
                         Syslog IP Address= ?
                         Log Facility= Local 1

                       Types:
                         CDR= No
                         Packet triggered= No
                         Filter Log= No
                         PPP Log= No


                     Press ENTER to Confirm or ESC to Cancel:

 Press Space Bar to Toggle.
```

Figure 10-7 Menu 24.3.2 — System Maintenance — Syslog and Accounting

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 10-3 System Maintenance Menu — Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter Log	No filters are logged when this field is set to **No**. Filters with the individual filter Log Filter field set to **Yes** are logged when this field is set to **Yes**.

Table 10-3 System Maintenance Menu — Syslog Parameters

PARAMETER	DESCRIPTION
PPP Log	PPP events are logged when this field is set to **Yes**.

The following are examples of the four types of syslog messages sent by the Prestige:

1 - CDR
SdcmdSyslogSend (SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)
C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
2 - Packet Triggered
SdcmdSyslogSend (SYSLOG PKTTRI, SYSLOG NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
3 - Filter Log
SdcmdSyslogSend (SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m), drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol (“TCP”, ”UDP”, ”ICMP”)
spo: Source port
dpo: Destination port
Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208]} S03>R01mF Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF
4 - PPP Log

```
SdcmdSyslogSend (SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP
Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing
```

10.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

```
                Menu 24.4 - System Maintenance - Diagnostic

xDSL                                    System
1.  Reset xDSL                          21. Reboot System
                                        22. Command Mode

TCP/IP
12. Ping Host


                          Enter Menu Selection Number:

                    Host IP Address= N/A
```

Figure 10-8 Menu 24.4 — System Maintenance — Diagnostic

Follow the procedure next to get to Diagnostic:

Step 1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.

Step 2. From this menu, type 4. Diagnostic to open **Menu 24.4** – **System Maintenance** – **Diagnostic**.

The following table describes the diagnostic tests available in menu 24.4 for and the connections.

Table 10-4 System Maintenance Menu — Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.

Chapter 11
Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

11.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a rom filename extension. Once you have customized the Prestige's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many ftp and tftp clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```
This is a sample ftp session showing the transfer of the computer file " firmware.bin" to the Prestige.

```
ftp> get rom-0 config.cfg
```
This is a sample ftp session saving the current configuration to the computer file config.cfg.

If your [t]ftp client does not allow you to have a destination filename different than the source, you will need to rename them as the Prestige only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or ftp site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version.

Table 11-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the Prestige.

11.2 Backup Configuration

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms “download” and “upload” are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

11.2.1 Backup Configuration Using FTP

Enter 5 in **Menu 24 - System Maintenance** to get the following screen.

```
                    Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, follow the
procedure below:


1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to your
   workstation.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must
remain in the menu to back up using TFTP), please see your router manual.


                              Press ENTER to Exit:
```

Figure 11-1 Menu 24.5 — Backup Configuration

11.2.2 Using the FTP command from the DOS Prompt

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open" and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter "root" and your SMT password as requested. The default is 1234.

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "get" to transfer files from the Prestige to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 11-2 FTP Session Example

The following table describes some of the commands that you may see in third party FTP clients.

Table 11-2 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

FTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

11.2.3 Backup Configuration Using TFTP

The Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next:

Step 1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the configuration file is `rom-0` (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the Prestige to the computer and "binary" to set binary transfer mode.

11.2.4 Example: TFTP Command

The following is an example tftp command:

```
TFTP [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige IP address, "get" transfers the file source on the Prestige (rom-0 name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

The following table describes some of the fields that you may see in third party TFTP clients.

Table 11-3 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Prestige and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

TFTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

11.3 Restore Configuration

Menu 24.6 -- System Maintenance - Restore Configuration allows you to restore the configuration via FTP or TFTP to your Prestige. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The Prestige restarts automatically after the file transfer is complete.

```
                    Menu 24.6 - Restore Configuration

To transfer the firmware and the configuration file, follow the procedure
below:


1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-spt is the
   Remote file name on the router. This restores the configuration to your
   router.
4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring using TFTP (note that you must
remain in the menu to back up using TFTP), please see your router manual.

                          Press ENTER to Exit:
```

Figure 11-3 Menu 24.6 — Restore Configuration

11.4 Uploading Firmware and Configuration Files

Menu 24.7 - System Maintenance - Upload Firmware allows you to upgrade the firmware and the configuration file.

WARNING!
PLEASE WAIT A FEW MINUTES FOR THE PRESTIGE TO RESTART AFTER FIRMWARE OR CONFIGURATION FILE UPLOAD. INTERRUPTING THE UPLOAD PROCESS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.

```
Menu 24.7 -- System Maintenance - Upload Firmware

     1. Upload System Firmware
     2. Upload System Configuration File


                Enter Menu Selection Number:
```

Figure 11-5 Menu 24.7 — System Maintenance — Upload Firmware

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

11.4.1 Firmware Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Prestige, you will see the following screens for uploading firmware and the configuration file using FTP.

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.


For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


                        Press ENTER to Exit:
```

Figure 11-6 Menu 24.7.1 — Upload System Firmware

11.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

```
          Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

                                  Press ENTER to Exit:
```

Figure 11-7 Menu 24.7.2 — System Maintenance

To transfer the firmware and the configuration file, follow these examples:

11.4.3 Using the FTP command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open” and the IP address of your Prestige.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter “root” and your SMT password as requested. The default is 1234.

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “put” to transfer files from the computer to the Prestige, e.g., put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the Prestige and renames it “ras”. Similarly “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the Prestige and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the Prestige to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the ftp prompt.

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 11-8 FTP Session Example

More commands that you may find in third party FTP clients, are listed earlier in this chapter.

FTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

11.4.4 TFTP File Upload

The Prestige also supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next:

Step 1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter the command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is “ras” and the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your

TFTP client program. For UNIX, use “get” to transfer from the Prestige to the computer, “put” the other way around, and “binary” to set binary transfer mode.

11.4.5 Example: TFTP Command

The following is an example tftp command:

```
TFTP [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the Prestige’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Prestige).

Commands that you may see in third party TFTP clients are listed earlier in this chapter.

TFTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

Chapter 12
System Maintenance and Information

This chapter leads you through SMT menus 24.8 to 24.10.

12.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information
3.  Log and Trace
4.  Diagnostic
5.  Backup Configuration
6.  Restore Configuration
7.  Firmware Update
8.  Command Interpreter Mode
9.  Call Control
10. Time and Date Setting
11. Remote Management



 Enter Menu Selection Number:
```

Figure 12-1 Command Mode in Menu 24

```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             config          ip
ppp             bridge          hdap
ras>
```

Figure 12-2 Valid Commands

12.2 Call Control Support

Call Control Support is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

```
                Menu 24.9 - System Maintenance - Call Control

                   1.  Budget Management



                        Enter Menu Selection Number:
```

Figure 12-3 Call Control

12.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 — System Maintenance — Call Control** to bring up the following menu.

```
                Menu 24.9.1 - System Maintenance - Budget Management

  Remote Node          Connection Time/Total Budget      Elapsed Time/Total Period
 1.ChangeMe                      No Budget                        No Budget
 2.--------                         ---                              ---
 3.--------                         ---                              ---
 4.--------                         ---                              ---
 5.--------                         ---                              ---
 6.--------                         ---                              ---
 7.--------                         ---                              ---
 8.--------                         ---                              ---

                          Reset Node (0 to update screen):
```

Figure 12-4 Budget Management

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node when PPPoE encapsulation is selected.

Table 12-1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter “0” to update the screen or press [ESC] to return to the previous screen.		

12.3 Time and Date Setting

The Prestige keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 — System Maintenance**, as shown next.

```
                Menu 24 - System Maintenance

                1.  System Status
                2.  System Information
                3.  Log and Trace
                4.  Diagnostic
                5.  Backup Configuration
                6.  Restore Configuration
                7.  Upload Firmware
                8.  Command Interpreter Mode
                9.  Call Control
                10. Time and Date Setting
                11. Remote Management

                Enter Menu Selection Number:
```

Figure 12-5 Menu 24 — System Maintenance

Then enter 10 to go to **Menu 24.10 — System Maintenance — Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

```
          Menu 24.10 - System Maintenance - Time and Date Setting


        Use Time Server when Bootup= None
        Time Server Address= N/A

        Current Time:                       00 : 00 : 00
        New Time (hh:mm:ss):                11 : 23 : 16

        Current Date:                       2000 - 01 - 01
        New Date (yyyy-mm-dd):              2001 - 03 - 01

        Time Zone= GMT

        Daylight Saving= No
        Start Date (mm-dd):                          01 - 00
        End Date (mm_dd):                            01 - 00

                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 12-6 Menu 24.10 System Maintenance — Time and Date Setting

Table 12-2 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None**. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

12.3.1 Resetting the Time

The Prestige resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the Prestige starts up, if there is a time server configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 13
IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

13.1 Introduction

Traditionally, routing is based on the destination address only and the IAD takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

13.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

13.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria includes the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, for example, telnet, tend to have short packets, while bulk traffic, for example, file transfer, tends to have large packets.

The actions that can be taken include:

- routing the packet to a different gateway (and hence the outgoing interface).
- setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

13.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

```
                Menu 25 - IP Routing Policy Setup

Policy                                  Policy
Set #          Name                     Set #          Name
------  -----------------               ------  -----------------
  1     test                              7     _________________
  2     _________________                 8     _________________
  3     _________________                 9     _________________
  4     _________________                10     _________________
  5     _________________                11     _________________
  6     _________________                12     _________________


                Enter Policy Set Number to Configure= 0

                Edit Name= N/A

                Press ENTER to Confirm or ESC to Cancel:
```

Figure 13-1 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

Step 1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup.**

Step 2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator “|” means the action is taken on criteria matched and separator “=” means the action is taken on criteria not matched.

```
                    Menu 25.1 - IP Routing Policy Setup

 # A                          Criteria/Action
 - - ------------------------------------------------------------------------
 1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
     SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
 2 N ____________________________________________________________________________
     ____________________________________________________________________________
 3 N ____________________________________________________________________________
     ____________________________________________________________________________
 4 N ____________________________________________________________________________
     ____________________________________________________________________________
 5 N ____________________________________________________________________________
     ____________________________________________________________________________
 6 N ____________________________________________________________________________
     ____________________________________________________________________________

Enter Policy Rule Number (1-6) to Configure:
```

Figure 13-2 Menu 25.1 — Sample IP Routing Policy Setup

Table 13-1 IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

```
                                Menu 25.1.1 - IP Routing Policy

          Policy Set Name= test
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Normal           Packet length= 40
            Precedence     = 0                  Len Comp= N/A
            Source:
              addr start= 1.1.1.1             end= 1.1.1.1
              port start= 20                  end= 20
            Destination:
              addr start= 2.2.2.2             end= 2.2.2.2
              port start= 20                  end= 20
          Action= Matched
            Gateway addr   = 192.168.1.1      Log= No
            Type of Service= Max Thruput
            Precedence     = 0

                              Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 13-3 IP Routing Policy

Table 13-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in **Menu 25 – IP Routing Policy Setup**.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or No to deactivate the policy. Inactive policies are displayed with a minus sign "-" in SMT menu 25.
Criteria	
IP Protocol	IP layer 4 protocol, for example, **UDP**, **TCP**, **ICMP**, etc.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput, Min Cost** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**,

Table 13-2 IP Routing Policy

FIELD	DESCRIPTION
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **No Change**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

13.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

13.5.1 Ethernet IP Policies

From **Menu 3 — Ethernet Setup**, type 2 to go to **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

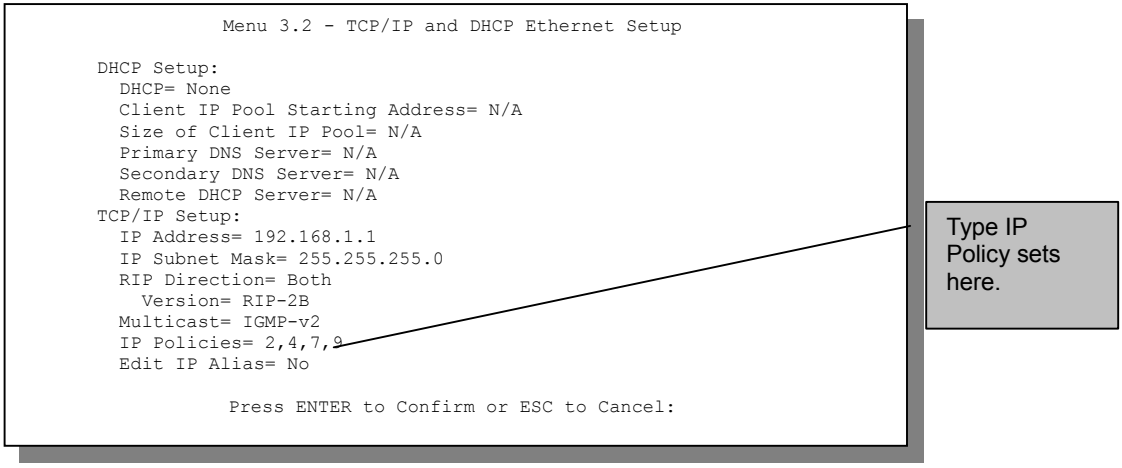
Menu 3.2 - TCP/IP and DHCP Ethernet Setup
DHCP Setup:
DHCP= None
Client IP Pool Starting Address= N/A
Size of Client IP Pool= N/A
Primary DNS Server= N/A
Secondary DNS Server= N/A
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies= 2,4,7,9
Edit IP Alias= No
Press ENTER to Confirm or ESC to Cancel:
Type IP Policy sets here.

Figure 13-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

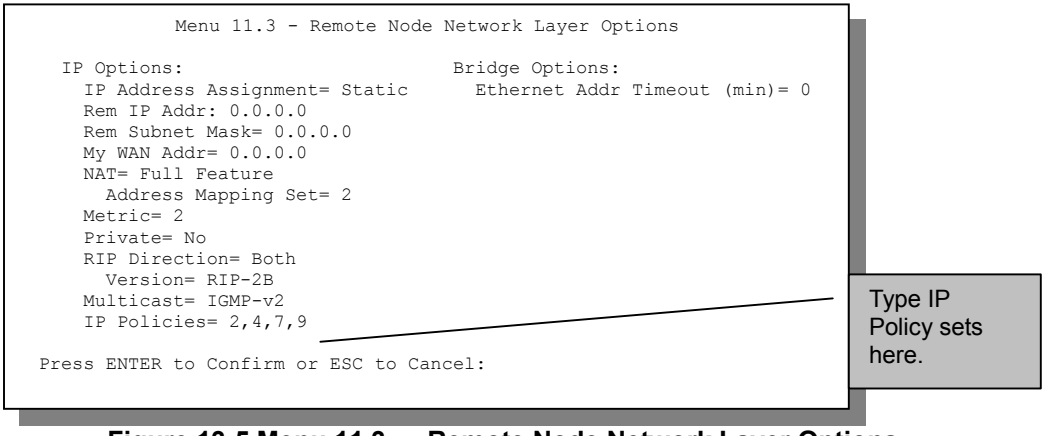

Figure 13-5 Menu 11.3 — Remote Node Network Layer Options

13.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

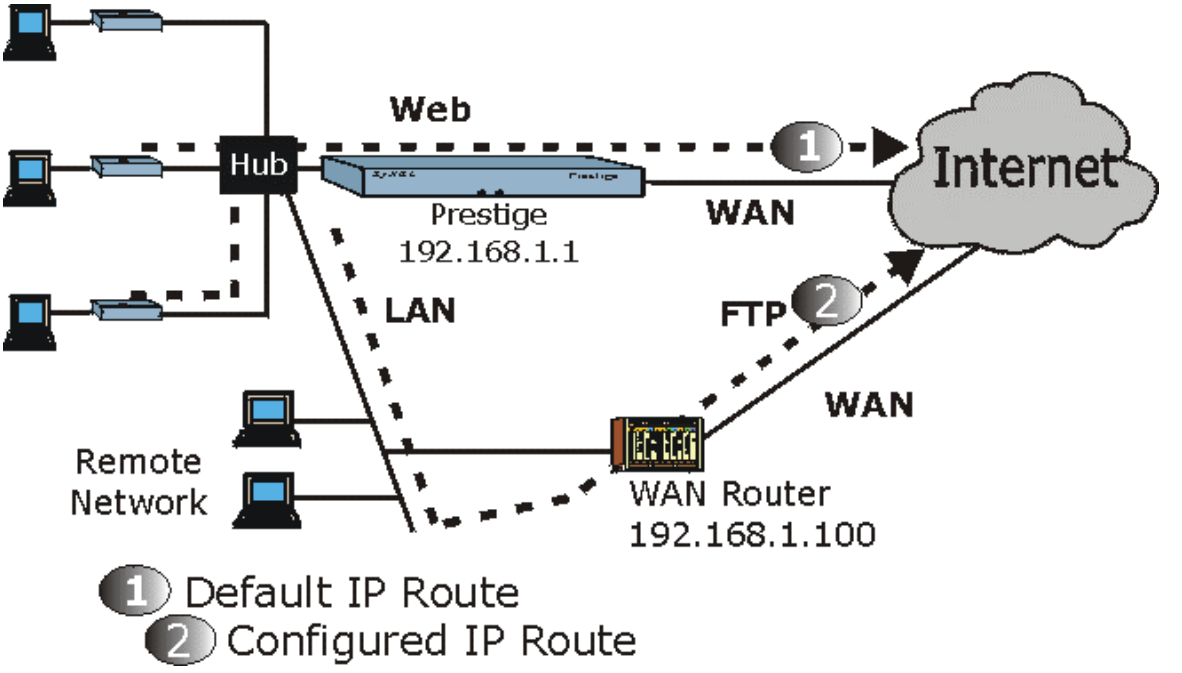

Figure 13-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

Step 1. Create a routing policy set in menu 25.

Step 2. Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.

```
                        Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria:
            IP Protocol     = 6
            Type of Service= Don't Care          Packet length= 10
            Precedence      = Don't Care           Len Comp= N/A
            Source:
              addr start= 192.168.1.2            end= 192.168.1.64
              port start= 0                      end= N/A
            Destination:
              addr start= 0.0.0.0                end= N/A
              port start= 80                     end= 80
          Action= Matched
            Gateway addr    = 192.168.1.1        Log= No
            Type of Service= No Change
            Precedence      = No Change

                   Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 13-7 IP Routing Policy Example

Step 3. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in menu 25.

Step 5. Create a rule in menu 25.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

```
                                Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set2

          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care             Packet length= 10
            Precedence     = Don't Care               Len Comp= N/A
            Source:
              addr start= 0.0.0.0                   end= N/A
              port start= 0                         end= N/A
            Destination:
              addr start= 0.0.0.0                   end= N/A
              port start= 20                        end= 21
          Action= Matched
            Gateway addr  =192.168.1.100            Log= No
            Type of Service= No Change
            Precedence     = No Change

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 13-8 IP Routing Policy

Step 6. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in menu 3.2 as shown next.

```
                      Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                        DHCP Setup
                          DHCP= Server
                          Client IP Pool Starting Address= 192.168.1.33
                          Size of Client IP Pool= 64
                          Primary DNS Server= 0.0.0.0
                          Secondary DNS Server= 0.0.0.0
                          Remote DHCP Server= N/A
                        TCP/IP Setup:
                          IP Address= 192.168.1.1
                          IP Subnet Mask= 255.255.255.0
                          RIP Direction= Both
                            Version= RIP-1
                          Multicast= None
                          IP Policies= 1,2
                          Edit IP Alias= No

                        Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Figure 13-9 Applying IP Policies

Chapter 14
Call Scheduling

Call scheduling (applicable for PPP or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

14.1 Introduction

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

```
                        Menu 26 - Schedule Setup

Schedule                                  Schedule
 Set #          Name                      Set #          Name
------   ----------------                 ------   ----------------
   1      ________________                   7      ________________
   2      ________________                   8      ________________
   3      ________________                   9      ________________
   4      ________________                  10      ________________
   5      ________________                  11      ________________
   6      ________________                  12      ________________

                  Enter Schedule Set Number to Configure=

                  Edit Name=

                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 14-1 Menu 26 — Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

```
                        Menu 26.1 - Schedule Set Setup

                Active= Yes
                Start Date(yyyy/mm/dd) = 2000 - 01 - 01
                How Often= Once
                Once:
                  Date(yyyy/mm/dd)= 2000 - 01 - 01
                Weekdays:
                  Sunday= N/A
                  Monday= N/A
                  Tuesday= N/A
                  Wednesday= N/A
                  Thursday= N/A
                  Friday= N/A
                  Saturday= N/A
                Start Time (hh:mm)= 00 : 00
                Duration (hh:mm)= 00 : 00
                Action= Forced On

                          Press ENTER to Confirm or ESC to Cancel:
      Press Space Bar to Toggle
```

Figure 14-2 Schedule Set Setup

If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 14-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes**
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	2000-01-01
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive.	**Once**

Table 14-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	EXAMPLE
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once**
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday : Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPP** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

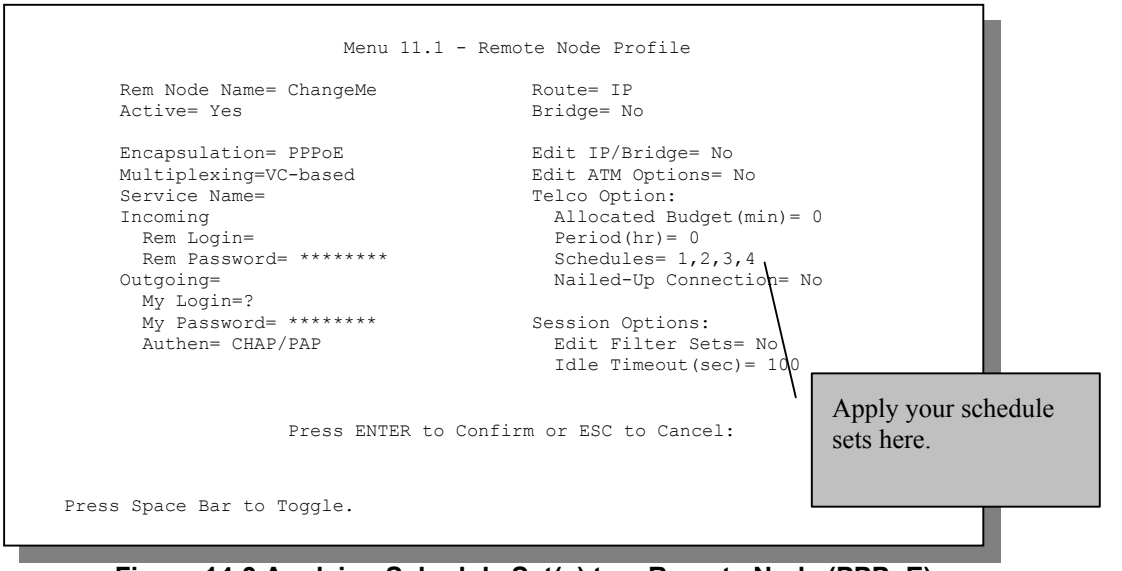

Figure 14-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Chapter 15
Remote Management

This chapter covers remote management (SMT menu 24.11).

15.1 Telnet

You can configure your Prestige for remote Telnet access as shown next.

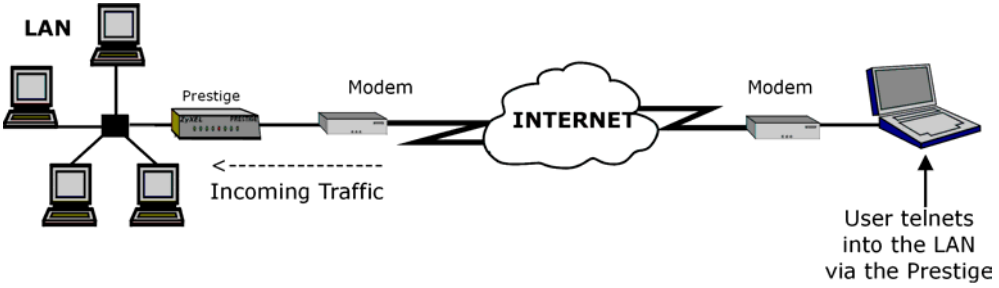

Figure 15-1 Telnet Configuration on a TCP/IP Network

15.2 FTP

You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

15.3 Web

You can use the Prestige's embedded web configurator for configuration and file management. See the *online help* for details.

15.4 Remote Management

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to display **Menu 24.11 — Remote Management Control**.

15.4.1 Remote Management Setup

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your Prestige from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

- WAN only (Internet)
- ALL (LAN and WAN)
- LAN only
- Disable (Neither)

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

Enter 11, from menu 24, to display **Menu 24.11 — Remote Management Control** (shown next).

```
                Menu 24.11 - Remote Management Control


TELNET Server:
  Server Port = 23                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

Figure 15-2 Menu 24.11 — Remote Management Control

Table 15-1 Menu 24.11 — Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service that you may use to remotely manage the Prestige.	
Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Access	Select the access interface (if any) by pressing the [SPACE BAR].	**LAN only**

Table 15-1 Menu 24.11 — Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.	**LAN only**
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

15.4.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
5. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

15.5 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

15.6 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your Prestige will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Part: IV

ADDITIONAL INFORMATION

This part contains Troubleshooting, Appendices and the Index.

Chapter 16
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

16.1 Problems Starting Up the Prestige

Table 16-1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adapter is connected to the Prestige and plugged in to an appropriate power source. Check that the Prestige and the power source are both turned on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

16.2 Problems with the LAN Interface

Table 16-2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN.	If the 10M/100M LEDs on the front panel are both off, check the Ethernet cable connections between your Prestige and computer. Check for faulty Ethernet cables. Make sure your NIC (Network Interface Card) is installed and functioning properly.
	Check the TCP/IP configuration on your computer. Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.

16.3 Problems with the WAN Interface

Table 16-3 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The WAN IP is provided when the ISP recognizes the user as an authorized user after verifying the MAC address, Host Name or User ID. Find out the verification method used by your ISP.
	If the ISP checks the host name, enter your computer's name in the **System Name** field in **Menu 1 — General Setup**.
	If the ISP checks the User ID, make sure that you have entered the correct service type, user name (in the **My Login** field) and password (in the **My Password** field) in **Menu 4 — Internet Access Setup**.
I cannot connect to a remote node or ISP.	Check menu 4 or menu 11.1 to verify the **Encapsulation** for the remote node.

16.4 Problems with Internet Access

Table 16-4 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet	Verify your settings in menu 3.2 and menu 4.
	Make sure the Prestige is turned on and connected to the network. If the Prestige's DSL LED is off, check the cable between the Prestige and the telephone wall jack. Make sure you entered your user name and password correctly. Your username may be case-sensitive.
Internet connection disconnects	Check the schedule rules in SMT menu 26. If you use PPP or PPPoE encapsulation, check the idle time-out setting in SMT menu 11.5. Contact your ISP.

16.5 Problems with the Password

Table 16-5 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the **Restore Factory Defaults/Reboot** button to restore the factory default configuration file. This will restore all of the factory defaults including the password. Refer to the *Resetting the Prestige* section in the *User's Guide* for details.

16.6 Problems with Telnet

Table 16-6 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN or WAN.	Refer to the *Remote Management Limitations* section for scenarios when remote management may not be possible.
	When NAT is enabled: ➢ Use the Prestige's WAN IP address when configuring from the WAN. ➢ Use the Prestige's LAN IP address when configuring from the LAN.
	Refer to the *Problems with the LAN Interface* section for instructions on checking your LAN connection.
	Refer to the *Problems with the WAN Interface* section for instructions on checking your WAN connection.

Appendix A
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the any expensive network cabling infrastructure. In effect a wireless LAN environment provides you the freedom to stay connected to the network while in the coverage area.

Benefits of a Wireless LAN

1. Access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. Doctors and nurses can access a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for networks that are frequently reconfigured.
4. Conference room users can access the network as they move from meeting to meeting- accessing up-to-date information that facilitates the ability to communicate decisions "on the fly".
5. It provides campus-wide networking coverage, allowing enterprises the roaming capability to set up easy-to-use wireless networks that transparently covers an entire campus.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs and to introduce a variety of performance improvements and benefits. On September 16, 1999, the 802.11b provided much higher data rates of up to 11Mbps, while maintaining the 802.11 protocol.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.

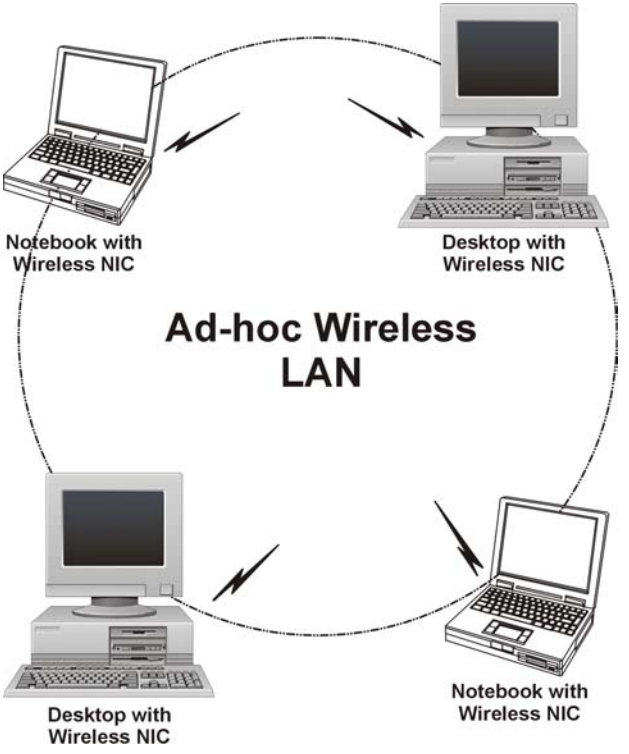

Diagram 1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access

points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an access point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.

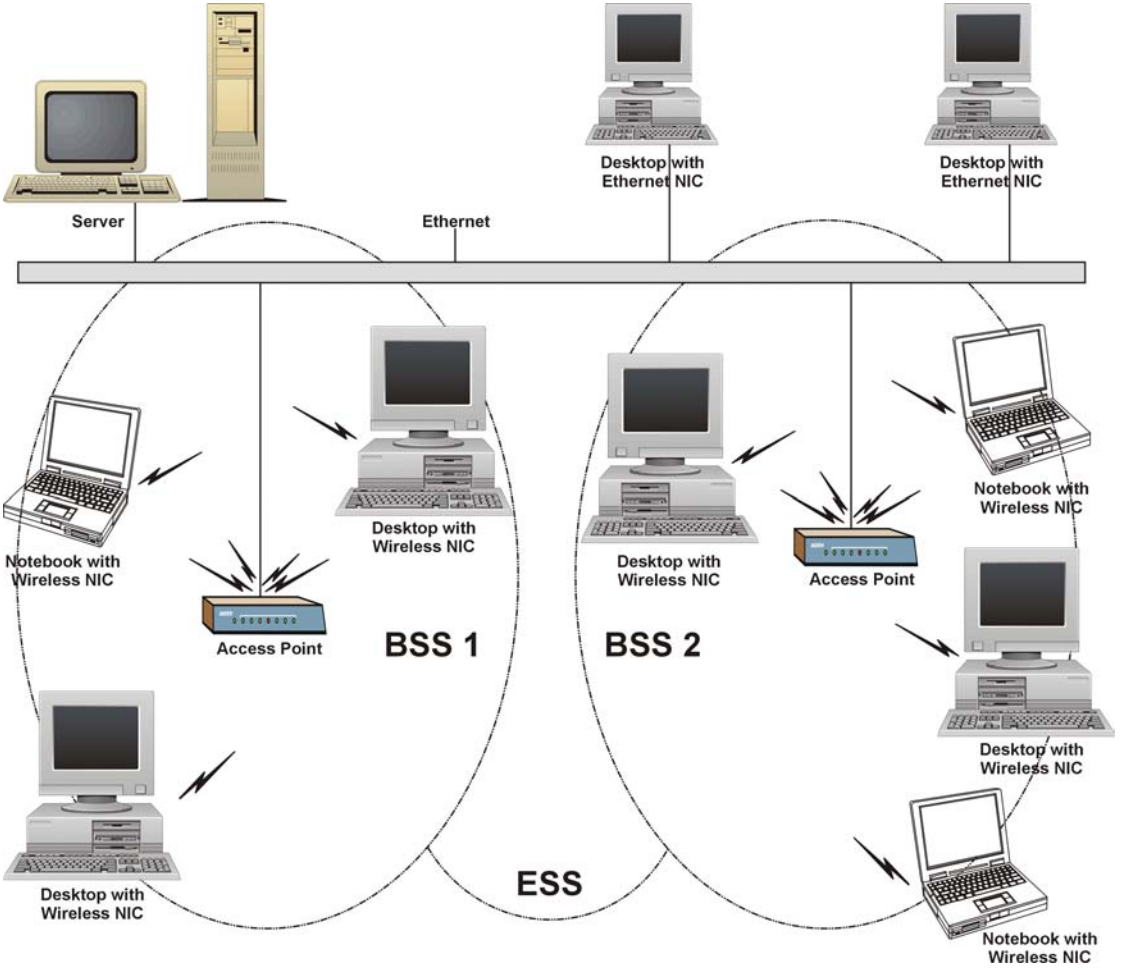

Diagram 2 ESS Provides Campus-Wide Coverage

Appendix B PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to a xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

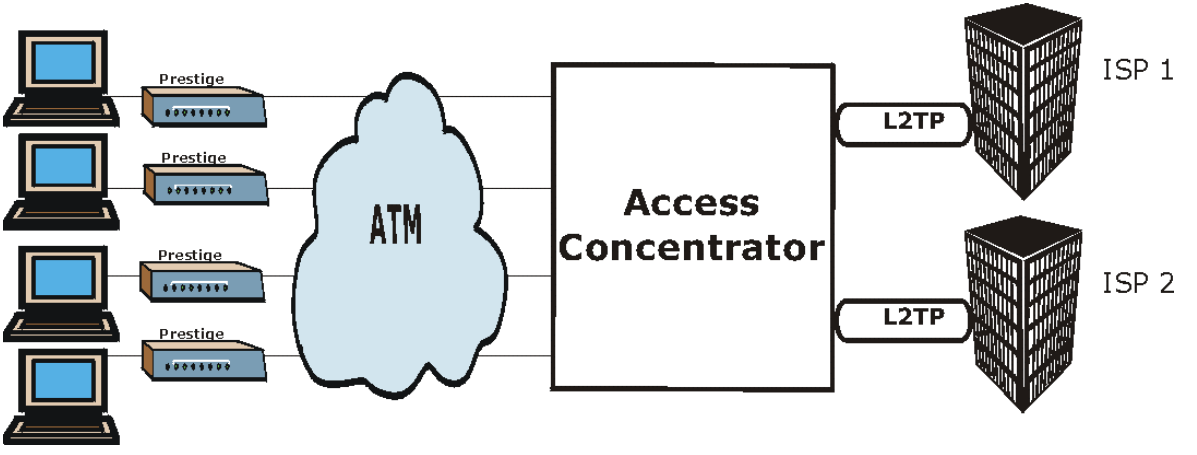

Diagram 3 Single-PC per Router Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

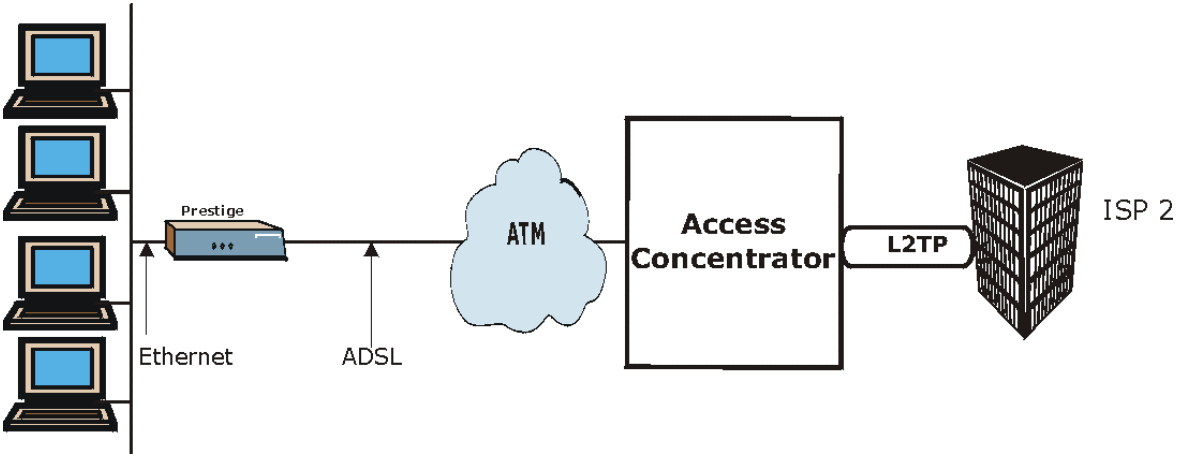

Diagram 4 Prestige as a PPPoE Client

Appendix C
Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel — Logical connections between ATM switches
- Virtual Path — A bundle of virtual channels
- Virtual Circuit — A series of virtual paths between circuit end points

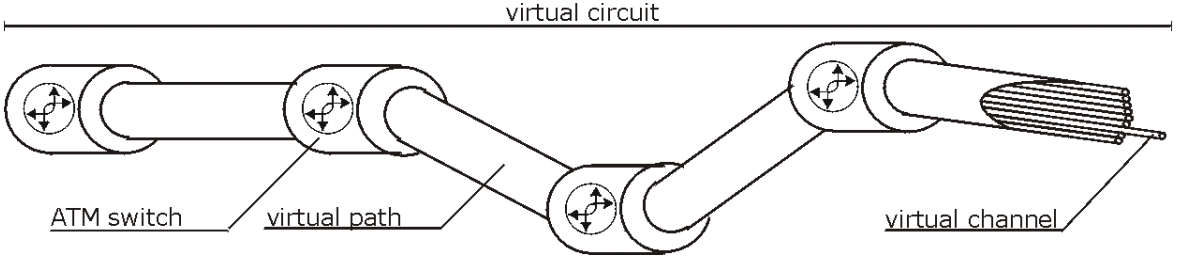

Diagram 5 Virtual Circuit Topology

Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Your service provider should supply you with VPI/VCI numbers.

Appendix D
Power Adapter Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-1215A
Input Power	AC120Volts/60Hz/30W
Output Power	AC12Volts/1.25A
Power Consumption	12 W
Safety Standards	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-121A25
Input Power	AC230Volts/60Hz/19W
Output Power	AC12Volts/1.25A
Power Consumption	12 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A3BN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.3A
Power Consumption	12 W
Safety Standards	TUV, CE (EN 60950)

Appendix E TCP/IP

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed. Use straight-through Ethernet cables to connect your computer's Ethernet adapter to a hub or switch and to connect the hub or switch to the Prestige's LAN port. Otherwise, connect your computer's Ethernet adapter directly to the LAN port with a crossover Ethernet cable.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

Setting up Your Windows 95/98/Me Computer

Installing TCP/IP Components

1. Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon.

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

e. Restart your computer so the changes you made take effect.

Configuring TCP/IP

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.
2. Click the **IP Address** tab.

   -If your IP address is dynamic, select **Obtain an IP address automatically**.

   -If you have a static IP address, select **Specify an IP address** and type your information into **the IP Address** and **Subnet Mask** fields.
3. Click the **DNS Configuration** tab.

   -If you do not know your DNS information, select **Disable DNS**.

   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).
4. Click the **Gateway** tab.

   -If you were not given a gateway IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway** field and click **Add**.
5. Click **OK** to save and close the **TCP/IP Pro**perties window.
6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7. Turn on your Prestige and restart your computer when prompted.

Verifying TCP/IP Properties

1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Setting up Your Windows NT/2000 Computer

Configuring TCP/IP

1. Click **Start**, **Settings**, **Network** and **Dial-up Connections** and right-click **Local Area Connection** or the connection you want to configure and click **Properties**.
2. Select **Internet Protocol (TCP/IP)** (you may need to scroll down) and click **Properties**.
3. The **Internet Protocol TCP/IP Properties** window opens.

   -If your IP address is dynamic, click **Obtain an IP address automatically**.

   -If you have a static IP address click Use the following IP Address and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
4. In the **Internet Protocol TCP/IP Properties** window:

   -Click **Obtain DNS server automatically** if you do not know your DNS server IP address(es).

   -If you know your DNS server IP address(es), type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS tab** to order them.
5. Click **Advanced**:

   -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.
6. Click **OK** to save and close the **Internet Protocol (TCP/IP) Properties** window.
7. Click **OK** to close the **Local Area Connection Properties** window.
8. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

Click **Start**, **Programs**, **Accessories** and then **Command Prompt**.

In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. The window will display information about your connection-specific DNS suffix, IP Address, Subnet Mask and Default Gateway.

Setting up Your Windows XP Computer

Configuring TCP/IP

1. Click **start**, **Control Panel**, **Network and Internet Connections** and then **Network Connections**.
2. Right-click the network connection you want to configure and then click **Properties**.
3. Under the **General** tab, select Internet Protocol (TCP/IP) (you may need to scroll down) and click **Properties**.
4. The **Internet Protocol TCP/IP Properties** window opens.

   -If you have a dynamic IP address click **Obtain an IP address automatically**.

-If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. To configure advanced static address settings for a local area connection, click **Advanced**, and do one or more of the following to configure additional IP addresses:

-In the **IP Settings** tab, in **IP addresses**, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

5. In the **Internet Protocol TCP/IP Properties** window's **General** tab:

-Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

-If you know your DNS server IP address(es), click Use the following DNS server addresses, type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

6. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
7. Click **OK** to close the **Local Area Connection Properties** window.
8. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support tab**.

Setting up Your Macintosh Computer

Configuring TCP/IP Properties

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.
2. Select **Ethernet** from the **Connect via** list.

3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

Check your TCP/IP properties in the **TCP/IP Control Panel**.

Index

A

Ad-hoc Configuration ..... B
ADSL, what is it? xviii
Authentication 4-5, 4-6
auto-negotiation 1-2

B

Back Panel
  connections description 2-3
backup 11-2
Basic Service Set ..... B
Bridging 2-17
  Ether Address 6-3
  Ethernet 6-1
  Ethernet Addr Timeout 6-2
  Remote Node 6-1
  Static Route Setup 6-2
BSS ..... See Basic Service Set
Budget Management 12-2, 12-3

C

Call Filtering 8-1
Call Filters
  Built-In 8-1
  User-Defined 8-1
Call Scheduling 14-1
  Maximum Number of Schedule Sets 14-1
  PPPoE 14-3
  Precedence 14-1
  Precedence Example ..... See precedence
CDR 10-6, 10-7
CDR (Call Detail Record) 10-6
Channel ID 3-13
CHAP 4-5
Clear to Send protocol 3-12
Collision 10-3
Command Interpreter Mode 12-1
Community 9-2
Computer Name 2-13
Connecting the Prestige 2-3
Connections
  Additional Requirements 2-4
  ADSL Line 2-3
  Power Adapter 2-4
  Rear Panel 2-2
Copyright ii
Cost Of Transmission 4-8, 5-5, 5-8
Country Code 10-4
CPU Load 10-3
CTS ..... See Clear to Send
Customer Support v

D

data collision 3-12
Data Filtering 8-1
Device Filter rules 8-16
DHCP 1-3, 10-5
Diagnostic 10-8
Diagnostic Tools 10-1
Digital Subscriber Line Access Multiplexer 1-6
Direct Sequence Spread Spectrum ..... A
Distribution System C
DNS 3-9
Domain Name 7-15
Domain Name System 3-4
DS ..... See Distribution System
DSL (Digital Subscriber Line) xviii
DSL, What Is It? xviii
DSLAM ..... See Digital Subscriber Line Access Multiplexer
DSSS ..... See Direct Sequence Spread Spectrum
Dynamic DNS 1-2, 2-14, 2-15
Dynamic Host Configuration Protocol 3-4
DYNDNS Wildcard 2-14

E

Encapsulation 1-4, 3-16, 3-21, 4-2

ENET ENCAP 3-16
PPP 3-17
PPP over Ethernet 3-17
RFC 1483 3-17
Error Log 10-5
Error/Information Messages
Sample 10-5
ESS ..... See Extended Service Set
ESS ID 3-11
Ethernet Encapsulation 7-14
Ethernet Traffic 8-20
Extended Service Set C

F

FCC iii
FHSS ... See Frequency-Hopping Spread Spectrum
Filename Conventions 11-1
Filter 2-17
Applying Filters 8-19
Ethernet traffic 8-20
Ethernet Traffic 8-20
Filter Rules 8-7
Filter Structure 8-4
Generic Filter Rule 8-14
Remote Node 4-9
Remote Node Filter 4-9
Remote Node Filters 8-20
Sample 8-18
SUA 8-16
TCP/IP Filter Rule 8-9
Filter Log 10-6, 10-7
Filter Rule 8-10
Filter Rule Process 8-3
Filter Rule Setup 8-9
Filter Rules Summary
Sample 8-19
Filter Set
Class 8-9
Filter Set Configuration 8-4
Filtering 8-1, 8-9
Filtering Process
Outgoing Packets 8-2
Fragment Threshold 3-14
Fragmentation Threshold 3-12
Frame Relay 1-6
Frequency-Hopping Spread Spectrum ..... A
FTP 15-3
Restrictions 15-3
FTP File Transfer 11-7
FTP Server 7-21
Full Rate 2-5

G

Gateway 5-8
Gateway Node 6-3
General Setup 2-13

H

Hidden Menus 2-11
Hidden Node problem 3-11
hop count 5-5
Hop Count 4-8, 5-8
HTTP 7-15

I

IANA 3-2, 3-3
IBSS ..... See Independent Basic Service Set
IEEE 802.11 ..... A
IEEE 802.11b 1-1
IGMP support 4-8, 5-5
Independent Basic Service Set ..... B
Infrastructure Configuration ..... B
Interactive Applications 13-1
Internet access 3-1
Internet Access ... 1-1, 1-2, 1-6, 2-12, 2-17, 3-1, 3-18, 3-20, 3-21
Internet Access Setup 7-6
Internet Assigned Numbers Authority .. See IANA
IP Address ... 3-10, 5-4, 5-8, 6-3, 8-11, 10-4, 10-8, 13-3
IP Address Assignment 3-17
ENET ENCAP 3-17

PPP or PPPoE 3-17
RFC 1483 3-17
IP Alias Setup 3-6
IP Filter 8-13
Logic Flow 8-12
IP mask 8-11
IP network number 3-2
IP Packet 8-14
IP Policies 13-5
IP Policy Routing (IPPR) 1-3, 3-5
Applying an IP Policy 13-5
Ethernet IP Policies 13-5
Gateway 13-5
IP Pool 3-4
IP Protocol 13-4
IP Routing Policy (IPPR) 13-1
Benefits 13-1
Cost Savings 13-1
Criteria 13-1
Load Sharing 13-1
Setup 13-2
IP Routing Policy Setup 13-3
IP Static Route 5-6
IP Static Route Setup 5-6, 5-7
ISDN 2-6

L

LAN 10-3
Link type 10-2
LLC-based Multiplexing 5-2
Log and Trace 10-5
Log Facility 10-6
Logging Option 8-11, 8-15
Login 4-5

M

MAC address 6-3
MAC Address Filter 3-15
MAC Address Filter Action 3-15
Main Menu 2-11
Management Information Base (MIB) 9-2
MBS ..... See Maximum Burst Size
Media Access Control 6-1
Message Logging 10-5
Metric 4-8, 5-5, 5-8
Multicast 4-8, 5-5
Multiplexing
LLC-based 3-16
VC-based 3-16
Multiplexing 1-4, 3-16, 3-21, 4-2
Multiprotocol Encapsulation 3-17
My WAN Address 4-8, 5-4

N

Nailed-Up Connection 4-3
NAT 8-16
Application 7-3
Applying NAT in the SMT Menus 7-6
Configuring 7-8
Definitions 7-1
Examples 7-18
How NAT Works 7-2
Mapping Types 7-4
Non NAT Friendly Application Programs 7-24
Ordering Rules 7-12
What NAT does 7-2
Network Address Translation 3-22
Network Address Translation (NAT) 7-1
Network Management 1-4

P

Packet
Error 10-2
Received 10-3
Transmitted 10-3
Packet Triggered 10-6, 10-7
Packets 10-2
PAP 4-5
Password 2-8, 2-13, 4-5, 9-2
Ping 10-8
Point-to-Point xviii
policy-based routing 13-1

POTS Splitter 2-5
PPP 4-2
PPP Encapsulation 5-2
PPP Log 10-7
Precedence 13-1, 13-4
Private 4-8, 5-5, 5-8
Protocol 8-10
Protocol Filter Rules 8-16

Q

Quality of Service 13-1

R

RAS 10-4, 13-2
Rate
  Receiving 10-2
  Transmission 10-2
Read Me First xvii
Related Documentation xvi
Remote DHCP Server 3-10
Remote Management Limitations 15-3
Remote Management Setup 15-1, 15-2
Remote Node 4-1, 10-2
  Remote Node Profile 4-4
  Remote Node Setup 4-1, 4-2
Remote Node Index Number 10-2
Remote Node Traffic 8-21
Request to Send protocol 3-12
Required fields 2-11
RESET Button 2-4
Restore Configuration 11-6
RF signals ..... A
RFC-1483 4-2
RFC-2364 ..... 4-2, 4-4
RIP ..... 3-10, 4-8, 5-5. See Routing Information Protocol
Routing Information Protocol 3-3
  Direction 3-3
  Version 3-3
Routing Policy 13-1
RTS ..... See Request to Send
RTS Threshold 3-11, 3-14

S

Sample IP Addresses 5-2
Schedule Sets
  Duration 14-2
SCR ..... See Sustain Cell Rate
Server 7-5, 7-8, 7-10, 7-13, 7-14, 7-15, 7-16, 7-19, 7-20, 12-5
Service iv
setup a schedule 14-2
SMT Menu Overview 2-9
SNMP
  Community 9-3
  Configuration 9-2
  Get 9-2
  Manager 9-2
  MIBs 9-2
  Trap 9-2
  Trusted Host 9-3
Source-Based Routing 13-1
Splitters 2-5
Static Route Setup 5-5
Static Routing Topology 5-6
STP 2-4
SUA 1-7
SUA (Single User Account) ..... See NAT
Subnet Mask 3-2, 3-10, 4-7, 5-4, 5-8, 10-4
Support Disk xvi
Supporting Disk xvi
Syntax Conventions xvii
Syslog 10-6
Syslog IP Address 10-6
Syslog Server 10-6
System
  Diagnostic 10-8
  Log and Trace 10-5
  Syslog and Accounting 10-6
  System Information 10-4
  System Status 10-1
System Information 10-3

System Information & Diagnosis 10-1
System Maintenance 10-1, 10-3, 11-2, 11-4, 11-6, 11-7, 11-9, 12-1, 12-2, 12-4
System Management Terminal 2-11
System Status 10-2
System Timeout 15-4

T

TCP/IP 5-1, 8-16, 10-8, 15-1
TCP/IP Options 5-1
TCP/IP Parameters 3-2
Telephone Microfilters 2-6
Telnet 15-1
Telnet Configuration 15-1
Telnet Under NAT 15-1
TFTP
  And FTP Over WAN} 15-3
  Restrictions 15-3
TFTP File Transfer 11-9
Time and Date Setting 12-4, 12-5
Time Zone 12-5
To avoid damage to the Prestige 2-4
TOS (Type of Service) 13-1
Trace Records 10-5
Transmission Rates ..... xvi, 1-1
Type of Service 13-1, 13-3, 13-4, 13-5

U

UNIX Syslog 10-5, 10-6
UNIX syslog parameters 10-6
Upload Firmware 11-6

V

VC-based Multiplexing 4-2, 5-1
VPI & VCI 3-16

W

WEP Encryption 3-14
WEP security 3-12
Wireless LAN ..... 3-11, A
  Benefits ..... A
Wireless LAN Setup 3-13
WLAN ..... See Wireless LAN

Z

ZyNOS 11-1, 11-2
ZyNOS F/W Version 11-1
ZyXEL Limited Warranty
  Note iv